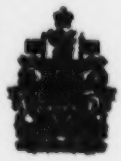
Privacy Commissioner of Canada



Commissaire à la protection de la vie privée du Canada

Your Privacy Responsibilities

A guide for businesses and organizations to Canada's *Personal Information Protection and Electronic Documents Act*

About This Guide

This guide helps businesses understand and meet their new obligations under Part 1 of the *Personal Information Protection and Electronic Documents Act*. *

The Act sets out ground rules for the management of personal information in the private sector.

It balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

The Act establishes the Privacy Commissioner of Canada as the ombudsman for complaints under the new law. The Commissioner seeks whenever possible to solve problems through voluntary compliance, rather than heavy-handed enforcement. The Commissioner investigates complaints, conducts audits, promotes awareness of, and undertakes research about privacy matters. The Commissioner is also the ombudsman for complaints under the *Privacy Act*, which covers the federal public sector.

Part I of the Act comes into force in three phases, beginning January 1, 2001.

For more information, contact:

The Privacy Commissioner of Canada
112 Kent Street
Ottawa ON K1A 1H3

Telephone: 1-613-995-8210
Toll-free: 1-800-282-1376
Fax: 1-613-947-6850
Web site: www.privcom.gc.ca
E-mail: info@privcom.gc.ca

While prepared with care to ensure accuracy and completeness, this guide has no legal status. For the official text of the new law, consult our web site at www.privcom.gc.ca or call the Office of the Privacy Commissioner.

Cette publication est également disponible en français.

*This guide deals only with Part I of the Act. All references to the Act in this document refer only to Part 1. Parts 2 to 5 of the Act concern the use of electronic documents and signatures as legal alternatives to original documents and signatures. For information on these, contact the Department of Justice.

A word from the Privacy Commissioner of Canada

The passage of the *Personal Information Protection and Electronic Documents Act* marks a significant step forward for Canada, putting it in the forefront of those nations embracing technological progress and electronic commerce while still protecting and enhancing long-cherished fundamental rights.

That Canadians are concerned about privacy, that they are enthusiastic about the new economy but cautious about their personal information, is old news. What businesses may find to be real news is that they themselves can benefit from observing the privacy principles and fair information practices set out in the *Personal Information Protection and Electronic Documents Act*. What the Act is really about is good information management practices, and every organization benefits from those. We've prepared this guide to help businesses appreciate what's required of them under the Act, and to help them get the full benefit of adopting the fair information practices that are the heart of the Act.

The Act is not unfailingly simple and straightforward—it is legislation, after all—though the principles it sets out are plain enough.

The Canadian Standards Association's *Model Code for the Protection of Personal Information*, which was developed by business in its own consultative process, is incorporated into the Act as an appendix (or, in the words of the legislative drafters, a Schedule). Reading the Act requires some jumping back and forth between the text of the statute proper and the text of the appended Code. I think the Act reflects the process of its creation, the hammering out of a consensus between business professionals, consumer advocates, and public policy experts. I also think businesses will find any inconveniences of the Act's structure a small price to pay for a system of regulation that reflects their input, their needs, the realities of their various ways of doing business. I'm hopeful that, for most businesses, the administration of the Act will feel more like self-regulation than government regulation. And, again, the privacy principles and fair information practices set out in the Act are not difficult to understand: they are good business practice, and they make good sense.

As you read the guide, you'll note the role played by my office: primarily a privacy ombudsman, determined to get to the bottom of problems and find solutions that work well for all parties. I take that role very seriously, and I want you to be assured that our oversight role includes giving help and advice to businesses searching for better ways to protect privacy. I'm looking forward to a vigorous, respectful relationship with business as we move into this new era of privacy protection. We all have a challenge, we all have much to learn—and we all have a great deal to gain.

This guide to the legislation is the work of many people and many months. I want to express my appreciation to the numerous private sector organizations that have donated their time and expertise to reviewing the guide at various stages of its development. Your advice and comments have been unfailingly thoughtful and practical.

I look forward to continuing this co-operative relationship as we work together to protect Canadians' right to privacy in the months and years ahead.

George Radwanski

Privacy Commissioner of Canada

Table of Contents

- The Act in Brief
- Is your organization subject to the Act?
- What is not covered by the Act?
- Your responsibilities under the Act
    1. Be accountable
    2. Identify the purpose
    3. Obtain consent
    4. Limit collection
    5. Limit use, disclosure and retention
    6. Be accurate
    7. Use appropriate safeguards
    8. Be open
    9. Give individuals access
    10. Challenging compliance
- Exceptions to the consent and access principles
- Role of the Privacy Commissioner
- Complaints to the Privacy Commissioner
- Applications to Federal Court
- Audits of personal information management practices
- Privacy Questionnaire

The Act in Brief

▲

Organizations covered by the Act must obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Personal information

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type
- opinions, evaluations, comments, social status, or disciplinary actions
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a

merchant, intentions (for example, to acquire goods or services, or change jobs)

Personal information does not include the name, title, business address or telephone number of an employee of an organization.

Complaints

An individual may complain to the organization in question or to the Privacy Commissioner about any alleged breaches of the law. The Privacy Commissioner may also initiate a complaint.

Application to the Federal Court

After receiving the Commissioner's investigation report, a complainant may apply to the Federal Court for a hearing under certain conditions as set out in Section 14 of the Act. The Privacy Commissioner may also apply to the Court on his own or on the complainant's behalf. The Court may order an organization to change its practices and/or award damages to a complainant, including damages for humiliation suffered.

Audits

The Privacy Commissioner may, with reasonable grounds, audit the personal information management practices of an organization.

Whistleblowing

Anyone who believes that any of Sections 5 to 10 of the Act have been or are about to be contravened may notify the Privacy Commissioner, and ask that his or her identity be kept confidential. Once the Privacy Commissioner has given his assurance, he is bound to protect the person's identity.

Offences

It is an offence to:

- destroy personal information that an individual has requested
- retaliate against an employee who has complained to the Privacy Commissioner, or who refuses to contravene Ssections 5 to- 10 of the Act
- obstruct a complaint investigation or an audit by the Privacy Commissioner or his delegate.

A person is liable to a fine of up to $10,000 on summary conviction or up to $100,000 for an indictable offence.

Definitions

Federal work, undertaking or business

Includes "any work, undertaking or business that is under the legislative authority of Parliament". While most federally regulated organizations would be captured under this definition, not all these types of organizations are federal works. For instance, insurance companies and credit unions may be subject to some federal regulation, but are considered to be within provincial jurisdiction under the Constitution and are not federal works for the purposes of the Act. The Act defines some of the specific federal works subject to Part 1 as follows:

- inter-provincial or international transportation by land or water
- airports, aircraft or airlines
- telecommunications
- radio and television broadcasting

- banks
- grain elevators
- nuclear facilities
- offshore drilling operations.

Note that this is not an exhaustive list of "federal works, undertakings and businesses". The fact that your company is federally incorporated does not necessarily mean that it is a federal work, undertaking or business. If your company is subject to any part of the *Canada Labour Code*, it is probably a federal work, undertaking or business.

Commercial activity

Any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists.

Organization

An organization includes an association, a partnership, a person and a trade union.

Consent

Voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure

Making personal information available to others outside the organization.

Use

Refers to the treatment and handling of personal information within an organization.

Is Your Organization Subject to the Act?

▲

The Act affects organizations in three stages:

January 1, 2001.

In its first stage, the Act applies to personal information (except personal health information) that is collected, used or disclosed in the course of commercial activities by federal works, undertakings and businesses. This includes, but is not limited to, federally-regulated organizations such as banks, telecommunications and transportation companies.

At this stage the Act also applies to personal data that is collected, used or disclosed by these same organizations about their employees.

In addition, at this stage the Act applies to disclosures of personal information for consideration across provincial or national borders, by organizations such as credit reporting agencies or organizations that lease, sell or exchange mailing lists or other personal information. The information itself must be the subject of the transaction and the consideration is for the information.

January 1, 2002

The Act extends to personal health information for the organizations and activities covered in the first stage. Personal health information is defined as information about an individual's mental or physical health, including information concerning health services provided and information about tests and examinations.

January 1, 2004

The Act extends to the collection, use or disclosure of personal information in the course of any commercial activity within a province. However, the federal government may exempt organizations and/or activities in provinces that have adopted substantially similar privacy legislation.

The Act will also apply to all personal information in all interprovincial and international transactions by all organizations subject to the Act in the course of their commercial activities.

Quebec is the only province that currently has legislation dealing with personal information in the privacy sector. The federal government has stated that this legislation meets the test of "substantially similar" and that organizations and activities subject to the Quebec legislation will be exempted from the federal act for intraprovincial matters.

Other provinces and territories are considering private sector legislation.

A Quick Test

Is your organization a federal work, undertaking or business that collects, uses or discloses personal information in the course of a commercial activity?

If YES, you are subject to the Act as of January 1, 2001. It also applies to your employees' personal information as well as your customers'.

If NO:
Do you disclose personal information outside the province for consideration? In other words, is personal information the subject of the transaction?

If YES, that disclosure is subject to the Act beginning January 1, 2001.

What is not Covered by the Act?

▲

- The collection, use or disclosure of personal information by federal government organizations listed under the *Privacy Act*
- Provincial or territorial governments and their agents
- An employee's name, title, business address or telephone number
- An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list)
- An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes

Your Responsibilities under the Act

Private sector organizations must follow a code for the protection of personal information, which is included in the Act as Schedule 1.

The code was developed by business, consumers, academics and government under the auspices of the Canadian Standards Association. It lists 10 principles of fair information practices, which form ground rules for the collection, use and disclosure of personal information. These principles give individuals control over how their personal information is handled in the private sector.

An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

The 10 principles that businesses must follow are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

These principles must be read in conjunction with key sections of the Act, including:

Sections 2 to 10 of the Act

Schedule 1 must be read in conjunction with sections 2 to 10 of the Act. It is essential to carefully consider the obligations set out in these sections, along with the ten principles.

Section 2

- Provides definitions including commercial activity, federal work, undertaking or business, personal information, personal health information and organization.
- Specifies that the notes under clauses 4.3 and 4.9 of Schedule 1 are not part of the law.

Section 3

Defines the purpose of the Act:

- recognizes individuals' right to privacy of their personal information
- recognizes the need of organizations to collect, use or disclose personal information for legitimate business purposes
- establishes rules for handling personal information

Section 4

Defines the scope of the Act's application:

- covers all organizations that collect, use or disclose personal information in the course of commercial activities

- includes the personal information of an employee of a federal work, undertaking or business but not the personal information of other private sector employees

Section 5

- Stipulates that every organization must comply with the obligations of Schedule 1
- Indicates what is not covered by the Act.
- In the Schedule:
  - "shall" means an obligation.
  - "should" means a recommendation, not an obligation.
- Limits the collection, use and disclosure to purposes that a reasonable person would consider appropriate in the circumstances. The reasonable person's perspective must be taken into account when applying any aspect of Part 1 of the Act.

Section 6

- Establishes that identifying an individual to be accountable for compliance does not mean that the organization is not responsible for its obligations as set out in Schedule 1.

Section 7

- Specifies the circumstances when personal information may be collected, used or disclosed without the individual's consent.

Section 8

- Sets out procedures for individuals to make requests for personal information and corrections to that information.

Section 9

- Explains when access to personal information may be refused.

Section 10

- Defines an organization's obligation to provide personal information in an alternative format (e.g. Braille, large print, or audio tape) to a person with a sensory disability.

Fair Information Principles

- The following section sets out the responsibilities for each of the 10 fair information principles of Schedule 1. It outlines how to fulfil these responsibilities and offers some tips.

The Reasonable Person

Section 5 of the Act limits the collection, use and disclosure for purposes that a "reasonable person" would consider appropriate in the circumstances.

Examples:

- Would a customer renting a movie from a video store consider it reasonable to be required to provide a telephone number? An address? A Social Insurance Number?
- Would a customer paying cash for a product or service consider it reasonable to be asked for a name, address and phone number?

1. Be accountable

▲

Your responsibilities

- Comply with all 10 of the principles of Schedule 1.
- Appoint an individual (or individuals) to be responsible for your organization's compliance.
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies and practices.

How to fulfil these responsibilities

- Give your designated privacy official senior management support and the authority to intervene on privacy issues relating to any of your organization's operations.
- Communicate the name or title of this individual internally and externally (e.g. on web sites and in publications).
- Analyze all personal information handling practices including ongoing activities and new initiatives, using the following checklist to ensure that they meet fair information practices:

  - What personal information do we collect?
  - Why do we collect it?
  - How do we collect it?
  - What do we use it for?
  - Where do we keep it?
  - How is it secured?
  - Who has access to or uses it?
  - To whom is it disclosed?
  - When is it disposed of?

- Develop and implement policies and procedures to protect personal information:

  - define the purposes of its collection,
  - obtain consent,
  - limit its collection, use and disclosure,
  - ensure information is correct, complete and current,
  - ensure adequate security measures,
  - develop or update a retention and destruction timetable,
  - process access requests, and
  - respond to inquiries and complaints.

- Include a privacy protection clause in contracts to guarantee that the third party provides the same level of protection as your organization does.
- Inform and train staff on privacy policies and procedures.
- Make information available explaining these policies and procedures to clients and customers (e.g. in brochures and on web sites).

Tips

Train your front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and process requests for access to personal information?
- To whom should I refer complaints about privacy matters?

- What are my privacy protections and rights? (This applies to employees in federally regulated organizations.)
- What are the ongoing activities and new initiatives relating to the protection of personal information at our organization?

When transferring personal information to third parties, ensure that they:

- Name a person to handle all privacy aspects of the contract.
- Limit use of the personal information to the purposes specified to fulfil the contract.
- Limit disclosure of the information to what is authorized by your organization or required by law.
- Refer any people looking for access to their personal information to your organization.
- Return or dispose of the transferred information upon completion of the contract.
- Use appropriate security measures to protect the personal information.
- Allow your organization to audit the third party's compliance with the contract as necessary.

2. Identify the purpose

▲

Your organization must identify the reasons for collecting personal information before or at the time of collection.

Your responsibilities

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it.

How to fulfil these responsibilities

- Review your personal information holdings to ensure they are all required for a specific purpose.
- Notify the individual, either orally or in writing, of these purposes.
- Record all identified purposes and obtained consents for easy reference in case an individual requests an account of such information.

Ensure that these purposes are limited to what a reasonable person would expect under the circumstances.

Tips

- Define your purposes for collecting data as clearly and narrowly as possible so the individual can understand how the information will be used or disclosed.
- Avoid overly broad purposes as they may conflict with the knowledge and consent principle.
- Examples of purposes include:

  - opening an account
  - verifying creditworthiness
  - providing benefits to employees
  - processing a magazine subscription
  - sending out association membership information
  - guaranteeing a travel reservation
  - identifying customer preferences
  - establishing customer eligibility for special offers or discounts

3. Obtain consent

▲

Your responsibilities

- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.
- Obtain the individual's consent before or at the time of collection, as well as when a new use is identified.

How to fulfil these responsibilities*

- Obtain consent from the individual whose personal information is collected, used or disclosed.
- Communicate in a manner that is clear and can be reasonably understood.
- Record the consent received (e.g. note to file, copy of e-mail, copy of checkoff box).
- Never obtain consent by deceptive means.
- Do not make consent a condition for supplying a product or a service, unless the information requested is required to fulfil an explicitly specified and legitimate purpose.
- Explain to individuals the implications of withdrawing their consent.
- Ensure that employees collecting personal information are able to answer an individual's questions about the purposes of the collection.

Tips

- Consent is normally obtained from the individual whose personal information is collected, used or disclosed.
- For an individual who is a minor, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian, or person having power of attorney.
- Consent is only meaningful if the individuals understand how their information will be used.
- Consent clauses should:

  - be easy to find
  - use clear and straightforward language
  - not use blanket categories for purposes, uses and disclosures
  - be specific as possible about which organizations handle the information

- Consent can be obtained in person, by phone, by mail, via the Internet etc.
- The form of consent should take into consideration:
  - reasonable expectations of the individual
  - circumstances surrounding the collection
  - sensitivity of the information involved
- Express consent should be used whenever possible and in all cases when the personal information is considered sensitive. Relying on express consent protects both the individual and the organization.

* There are some exceptions to the principle of obtaining consent.

Grandfathering

Personal information that your company has collected during the course of its commercial activities is subject to the Act. Since it has already been collected, you don't need to recollect it. However, in order to continue to use or disclose this information, you now require consent. Some organizations have informed all their

customers what they do with their information, to whom it is disclosed and given customers the option to object to these ongoing uses or disclosures.

4. Limit collection

▲

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfil these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Identify the kind of personal information you collect in your information-handling policies and practices.
- Ensure that staff members can explain why the information is needed.

Tips

- By reducing the amount of information gathered, you can lower the cost of collecting, storing, retaining and ultimately archiving data.
- Collecting less information also reduces the risk of inappropriate uses and disclosures.

5. Limit use, disclosure and retention

▲

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

How to fulfil these responsibilities

- Document any new purpose for the use of personal information.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- Dispose of information that does not have a specific purpose or that no longer fulfils its intended purpose.
- Dispose of personal information in a way that prevents improper access. Shredding paper files or deleting electronic records are ideal.
- Establish policies setting out the types of information that need to be updated. An organization can reasonably expect an individual to provide updated information in certain circumstances (e.g. change of address for a magazine subscription).

Tips

- It may be less onerous and complicated to destroy or erase information than to make personal information anonymous.
- Conduct regular reviews to help determine whether information is still required. Establish a retention schedule to make this easier.

6. Be accurate

▲

Your responsibilities

Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

How to fulfil these responsibilities

- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual.
- Update personal information only when necessary to fulfil the specified purposes.
- Keep frequently used information accurate and up to date unless there are clearly set out limits to this requirement.

Tips

- One way to determine if information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would harm the individual.
- Apply the following checklist for accuracy:

  - List specific items of personal information required to provide a service.
  - List the location where all related personal information can be retrieved.
  - Record the date when the personal information was obtained or updated.
  - Record the steps taken to verify accuracy, completeness and timeliness of the information.

  This may require reviewing your records or communicating with the client.

7. Use appropriate safeguards

▲

Your responsibilities

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

How to fulfil these responsibilities

- Develop and implement a security policy to protect personal information.
- Use appropriate security safeguards to provide necessary protection:

  - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
  - technological tools (passwords, encryption, firewalls, anonymizing software)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, confidentiality agreements)

- Make your employees aware of the importance of maintaining the security and confidentiality of personal information.
- Ensure staff awareness by holding regular staff training on security safeguards.
- The following factors should be considered in selecting appropriate safeguards:

  - sensitivity of the information
  - amount of information
  - extent of distribution
  - format of the information (electronic, paper, etc.)
  - type of storage.

- Review and update security measures regularly.

Tips

- Make sure personal information that has no relevance to the transaction is either removed or masked when providing copies of information to others.
- Keep sensitive information files in a secure area or computer system and limit access to individuals on a "need-to-know" basis only.

8. Be open

▲

Your responsibilities

- Inform customers, clients and employees that you have policies and practices for the management of personal information.
- Make these policies and practices understandable and easily available.

How to fulfil these responsibilities

- Ensure front-line staff is familiar with the procedures for responding to individual inquiries.
- Make the following available:

  - name or title and address of the person who is accountable for your organization's privacy policies and practices
  - name or title and address of the person to whom access requests should be sent
  - how an individual can gain access to his or her personal information
  - how an individual can complain to your organization
  - brochures or other information that explain your organization's policies, standards or codes
  - a description of what personal information is made available to other organizations (including subsidiaries) and why it is disclosed.

Tip

- Information about these policies and practices may be made available in person, in writing, by telephone, in publications or on your organization's web site.

9. Give individuals access

Your responsibilities

- When requested, inform individuals if you have any personal information about them.
- Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.
- Give individuals access to their information.
- Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act (see below).
- An organization should note any disagreement on the file and advise third parties where appropriate.

How to fulfil these responsibilities

- Provide any help the individual needs to prepare a request for access to personal information.
- Your organization may ask the individual to supply enough information to enable you to account for the existence, use and disclosure of personal information.
- Respond to the request as quickly as possible and no later than 30 days after receipt of the request.
- The normal 30-day response time limit can be extended for a maximum of 30 additional days, according to specific criteria set out at Subsection 8(4) of the Act:

  - if responding to the request within the original 30 days would unreasonably interfere with activities of your organization
  - if additional time is necessary to conduct consultations
  - if additional time is necessary to convert personal information to an alternate format

- If your organization extends the time, you must notify the individual making the request within 30 days of receiving the request, and of his or her right to complain to the Privacy Commissioner.
- Give access at minimal or no cost to the individual.
- Notify the individual of the approximate costs before processing the request.
- Give individuals access to their personal information.
- Make sure the requested information is understandable. Explain acronyms, abbreviations and codes.
- Send any information that has been amended, where appropriate, to any third parties that have access to the information.
- Inform the individual in writing when refusing to give access, setting out the reasons and any recourse available.
- There are some exceptions to the principle of providing access.

Tips

- Keep personal information about individuals in one place to make retrieval easier. Or record where all such information can be found.
- Never disclose personal information unless you are sure of the identity of the requestor and that person's right of

access.
- If you do not store all personal information in one place, keep a record of where the information can be found to make retrieval easier.

10. Challenging compliance

Your responsibilities

- Develop simple and easily accessible complaint procedures.
- Inform complainants of avenues of recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

How to fulfil these responsibilities

- Record the date a complaint is received and the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention).
- Acknowledge receipt of the complaint promptly.
- Contact the individual to clarify the complaint, if necessary.
- Assign the investigation to a person with the skills necessary to conduct it fairly and impartially.
- Give the investigator access to all relevant records, employees or others who handled the personal information or access request.
- Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of complaints.

Tips

- How well your organization handles an individual's complaint may help preserve or restore the individual's confidence in your organization.
- Record all decisions to ensure consistency in applying the Act.

Exceptions to the Consent and Access Principles

There are a number of exceptions to the requirements to obtain consent and provide access set out in the Act.

Exceptions to consent in Section 7

Organizations may *collect* personal information without the individual's knowledge or consent only:

- if it is clearly in the individual's interests and consent is not available in a timely way
- if knowledge and consent would compromise the availability or accuracy of the information **and** collection is required to investigate a breach of an agreement or contravention of a federal or provincial law
- for journalistic, artistic or literary purposes
- if it is publicly available as specified in the regulations.

Organizations may *use* personal information without the individual's knowledge or consent only:

- if the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law **and** the information is used for that investigation
- for an emergency that threatens an individual's life, health or security
- for statistical or scholarly study or research (the organization must notify the Privacy Commissioner before using the information)
- if it is publicly available as specified in regulations
- if the use is clearly in the individual's interest and consent is not available in a timely way
- if knowledge and consent would compromise the availability or accuracy of the information **and** collection was required to investigate a breach of an agreement or contravention of a federal or provincial law.

Organizations may *disclose* personal information without the individual's knowledge or consent only:

- to a lawyer representing the organization
- to collect a debt the individual owes to the organization
- to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction
- to a government institution that has requested the information, identified its lawful authority, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law
- to an investigative body named in the Regulations of the Act or government institution on the organization's initiative when the organization believes the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or suspects the information relates to national security or the conduct of international affairs
- if made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law
- in an emergency threatening an individual's life, health, or security (the organization must inform the individual of the disclosure)
- for statistical, scholarly study or research (the organization must notify the Privacy Commissioner before disclosing the information)
- to an archival institution
- 20 years after the individual's death or 100 years after the record was created
- if it is publicly available as specified in the regulations
- if required by law.

Exception to access in Section 9

Organizations *must* refuse an individual access to personal information:

- if it would reveal personal information about another individual* unless there is consent or a life-threatening situation
- if the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations *may* refuse access to personal information if the information falls under one of the following:

- solicitor-client privilege
- confidential commercial information *
- disclosure could harm an individual's life or security *
- it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified)

- it was generated in the course of a formal dispute resolution process.

• If this information can be removed, the organization must release the remaining information.

Role of the Privacy Commissioner

The Privacy Commissioner of Canada has oversight of both the *Privacy Act* and Part 1 of the *Personal Information Protection and Electronic Documents Act*. These acts protect personal information according to internationally accepted fair information principles and practices.

The Commissioner is an Officer of Parliament, like the Auditor General of Canada or the Chief Electoral Officer. As an Officer of Parliament, the Commissioner reports directly to the House of Commons and to the Senate, not to the government of the day. This independence ensures his impartiality and open-mindedness in exercising his role as an ombudsman for privacy matters. The Commissioner makes recommendations, not orders. However there is provision to apply to the Federal Court to review a case.

The Privacy Commissioner: a privacy ombudsman

Nearly two decades of experience investigating complaints under the *Privacy Act* have helped define the Privacy Commissioner's ombudsman role. The Privacy Commissioner relies on the competence, knowledge and impartiality of his staff to seek whenever possible to resolve disputes through investigation, persuasion, mediation and conciliation. Ideally this approach to resolving disputes can be less intimidating to complainants and less costly to business than recourse to the courts. While the Commissioner protects individual rights, he is also an advocate for the fair information principles that form the foundation of the legislation. The Commissioner's thorough investigations and impartiality protect both individual rights and the organization against unfair accusations.

Specific responsibilities under the Act

The Act makes the Privacy Commissioner responsible for ensuring compliance with the Act and for promoting its purposes.

Compliance roles

The Commissioner has five main ways of ensuring that organizations subject to the Act adhere to its principles:

- investigating complaints
- mediating and conciliating complaints
- auditing personal information management practices
- publicly reporting abuses
- seeking remedies in court.

(See **Complaints to the Privacy Commissioner**, and **Audits of Personal Management Practices**)

Promoting the purposes of the Act

The Commissioner promotes the purposes of the Act in four ways:

- education
- research
- reporting
- consultation and agreements.

Education

The Commissioner's education mandate includes developing and conducting public information programs to encourage and promote understanding of privacy issues.

Research

The Act requires the Commissioner to undertake and publish research about protecting personal information so as to increase knowledge and improve compliance with the Act's fair information principles. The Commissioner may conduct independent research on privacy issues in conjunction with academic or other researchers. He may also provide grants and contributions for academic or other research on privacy issues.

Reporting

The Commissioner may make public any information about an organization's personal information management practices, if he considers it in the public interest. He reports annually to Parliament on privacy issues including the extent to which provinces have introduced similar legislation.

Consultation and agreements

The Commissioner may enter into agreements with provincial counterparts who have similar powers and duties. These consultations and agreements may cover complaint mechanisms, research, and developing model contracts for protecting personal information. The Commissioner will encourage organizations to develop detailed policies and practices to comply with Part 1 of the Act.

Complaints to the Privacy Commissioner

▲

Types of complaints

An individual may complain to the Commissioner about any matter specified in sections 5 to10 of the Act or in the recommendations or obligations set out in Schedule 1. This includes but is not limited to allegations that an organization:

- denies an individual access to personal information
- improperly collects, uses or discloses personal information
- refuses to correct inaccurate or incomplete information
- fails to provide access to personal information in an alternative format to an individual with a sensory disability
- does not use appropriate safeguards to protect personal information.

The Commissioner may initiate a complaint if there are reasonable grounds to believe that an investigation of a matter under Part 1 of the Act is warranted.

Time limits

There is no time limit for filing most types of complaints.

The only exception is a complaint that access to personal information has been denied. In this case, the complaint must be made within six months after the organization's refusal to provide the information, or after the expiry of the time limit for responding to the request. However, the Commissioner may extend the time limit for an access complaint.

The Commissioner has one year from the date of the complaint to prepare a report.

How does the Privacy Commissioner handle complaints?

As an ombudsman, the Commissioner seeks to take a cooperative and conciliatory approach to investigations whenever

possible. He encourages the resolution of complaints through negotiation and persuasion. Alternate dispute resolution methods such as mediation and conciliation may be used to settle matters at any stage of the investigation process. Although the Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence, these means are only likely to be used if voluntary cooperation is not forthcoming.

At the outset of an investigation, the Commissioner will notify the organization in writing of the substance of the complaint and will identify the investigator responsible for the case. The organization may submit representations to the Commissioner at any time during the process.

The investigator assigned to the case will contact the organization's designated staff member to indicate how he or she intends to proceed with the investigation and, if possible, which records need to be reviewed and which staff members may be interviewed. The investigator may also indicate whether on-site visits will be needed.

Investigators obtain information directly from individuals familiar with the matter under investigation. These interviews are conducted in private. Investigators may also require access to original documents. Documents given to an investigator are returned within 10 days of a request for their return, but they may be asked for again if the need arises.

Prior to finalizing the investigation, the results are disclosed to the parties involved. They may make additional representations if they see fit. This also gives them the opportunity to resolve the matter before the complaint is finalized.

The investigator submits the results of the investigation to the Commissioner along with any representations. The Commissioner will consider the case and issue a report to the parties. The Commissioner can request that an organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement report recommendations, or explain why no action has or will be taken. The report includes the results of the investigation, any settlement reached by the parties, recommendations such as suggested changes in information management practices, what steps the organization has taken or will take to address these recommendations and, if applicable, notice of recourse to the Federal Court.

A complaint may be disposed of in one of the following three ways:

1. Not well founded

There is no evidence to lead the Commissioner to conclude that the organization violated the Act.

2. Well founded

The investigation revealed that the organization failed to respect a provision of the Act and the complaint was not resolved.

3. Resolved

The investigation supports the complaint, but the organization agrees to take corrective action to remedy the situation. For example, the organization agrees to release personal information previously denied.

The complaint may also be resolved if it appears to be the result of miscommunication or misunderstanding. For example, an organization misunderstood the request and now agrees to release the personal information sought by the complainant.

The complaint is also resolved if the complainant is satisfied with the Commissioner's efforts and the results.

The Commissioner is not required to issue an investigation report if:

- the complainant has not pursued alternate redress mechanisms that are reasonably available;
- the case could be more appropriately dealt with through other legislation;
- too much time has passed since the matter that prompted the complaint and reporting would serve no useful purpose; or,
- the complaint is trivial, frivolous or vexatious, or is made in bad faith.

Public disclosure

The Privacy Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

Applications to Federal Court

A complainant may apply to the Federal Court for a hearing. The Privacy Commissioner may apply on his own or on a complainant's behalf. Normally, an application must be made within 45 days of the Commissioner's report.

What Matters Can Be Heard

The Court will consider applications arising from the complaint or any matter referred to in the Commissioner's report and that is referred to in one of the following

Under Schedule 1

4.1.3 Whether an organization has properly exercised its responsibility for the personal information in its possession including information transferred to a third party.

4.2 Whether an organization has properly identified and documented the purposes for which personal information is being collected, used or disclosed, at or before the time of collection.

4.3.3 Whether an organization has refused to provide a service to an individual because the individual would not consent to the collection, use or disclosure of more information than necessary for the specified purpose.

4.4 Whether an organization has collected more information than necessary for the purposes or whether it was collected by fair and lawful means.

4.6 Whether the information is accurate, up-to-date and complete as necessary.

4.7 Whether an organization has taken the necessary steps to safeguard the information.

4.8 Whether an organization has made specific information about its personal information management policies readily available to individuals.

Under Schedule 1 as modified by Sections 5 to 10 of the Act

4.3 Whether personal information has been collected, used or disclosed without the knowledge or consent of the individual, except where permitted or required.

4.5 Whether an organization has used or disclosed personal information for purposes other than those for which it was collected, without the consent of the individual and in circumstances not authorized by the Act. As well, whether an organization has retained the information long enough for a complainant to exhaust his remedies under the Act.

4.9 Whether an individual was wrongly denied access to information about himself except where permitted or required.

Sections of the Act

5(3) Whether the information was collected, used or disclosed only for purposes that a reasonable person would consider appropriate.

8(6) Whether an individual has been charged too much for access to information or was not notified in advance of the cost.

8(7) Whether an organization has informed the individual in writing of a refusal to give access, has given the reasons for the refusal and set out the appropriate recourse available.

10 Whether an organization has failed to grant access in an alternative format to an individual with a sensory disability.

Remedies available through Federal Court

The Federal Court may order an organization to correct practices that do not comply with Sections 5 to 10 of the Act. The Court may also order an organization to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on monetary damages that the Court may award.

Audits of Personal Information Management Practices

▲

The Act gives the Privacy Commissioner the authority to audit an organization's personal information management practices when he has reasonable grounds to believe the organization is not fulfilling its obligations under Part 1 of the Act or is not respecting the recommendations of Schedule 1.

What can lead to an audit?

The following are examples of circumstances that may lead the Commissioner to audit the personal information management practices of an organization:

- a group or series of complaints about a particular organization's practice(s)
- information provided by an individual under the whistleblower provision
- an issue receiving media attention.

What to expect from an audit by the Privacy Commissioner

In keeping with the Commissioner's ombudsman approach, privacy audits are non-confrontational, whenever possible, and can be useful for organizations wanting to improve their personal information handling practices.

The Commissioner will inform the organization in writing that an audit will be undertaken. The letter will specify the audit's focus, propose a reasonable timeframe, and name the officer delegated to conduct the audit.

Although the Commissioner has the power to summon witnesses, administer oaths and compel organizations to produce evidence, audits are unlikely to be conducted on such a formal basis unless voluntary cooperation is not forthcoming.

The officer will meet with the organization's representative for a preliminary discussion of the intent, purpose and scope of the review.

When the officer requires access to any of the organization's premises, he or she will satisfy security requirements. The officer may interview any person in private on the premises, examine records and obtain copies or extracts of such records. The officer will return any document within 10 days of a request for their return but may ask for them again if the need arises.

Once the audit is finished, the officer will debrief the organization's representative on the findings. The officer will report the audit findings to the Commissioner who will make recommendations. The Commissioner will send the report to the organization and may ask to be kept informed of actions the organization takes to correct problems.

The Commissioner may include the audit report in his annual report or he may make public the personal information management practices of an organization if he considers it to be in the public interest to do so.

Privacy Questionnaire

The following are some common sense questions you can use to help your organization prepare for implementation of the *Personal Information Protection and Electronic Documents Act*. The following questionnaire may be used along with the description of the Act in this guide.

If you are unsure about whether or when the Act applies to your organization, please refer to the section on *Is your organization subject to the Act* of this guide.

Not all of the following questions will apply to all organizations, as the Act applies to a wide variety and size of organizations. Consider each question along with your organization's current practices. Answering "no" indicates areas that need to be addressed or improved.

Personal information holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept (electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

Accountability of organization and staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
    - requests for personal information?
    - requests for correction?
    - complaints from the public?
- Do your customers know whom to contact:
    - for general inquiries regarding their personal information?
    - to request their personal information?
    - to request corrections to their personal information?
    - for complaints?
- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?
- Will there be ongoing training?
- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?
- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

Information for customers and employees

- Do you have documents that explain your personal information practices and procedures to your customers?
- Does this information include how to:
  - obtain personal information?
  - correct personal information?
  - make an inquiry or complaint?
- Does this information describe personal information that is:
  - held by the organization and how it is used?
  - disclosed to subsidiaries and other third parties?
- Do you have a privacy policy for your web site?
- Is your privacy policy prominent and easy to find? Is it easily understandable?
- Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- Have you ensured that the public can obtain this information easily and without cost?
- Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

Limiting collection, use, disclosure and retention to identified purposes

- Have you identified the purposes for collecting personal information?
- Are these purposes identified at or before the time the information is collected?
- Do you collect only the personal information needed for identified purposes?
- Do you document the purposes for which personal information is collected?
- If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- Have you developed a timetable for retaining and disposing of personal information?
- When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

Consent

- Does your staff know that an individual's consent must be obtained before or at the time they collect personal information?
- Does your staff know they must obtain an individual's consent before any new use or new disclosure of the information?
- Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?
- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

Third party transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party's use of information to purposes necessary to fulfil the contract?
- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

Ensuring accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your

organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
  - sensitivity of the information?
  - scale of distribution?
  - format of the information?
  - method of storage?
- Have you developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?
- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

Requests for access to personal information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?
- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

Handling complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?
- Are your customer assistance and other front-line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?
- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome?

CLOSE

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Protection des renseignements personnels : vos responsabilités

Loi sur la protection des documents personnels et les documents électroniques du Canada
Guide à l'intention des entreprises et des organisations

À propos du présent guide

Le présent guide a pour but d'aider les entreprises à comprendre leurs obligations en vertu de la Partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* *, et à s'y conformer.

La Loi définit des règles de base au sujet de la gestion des renseignements personnels dans le secteur privé. Elle établit un équilibre entre le droit d'un particulier à la protection des renseignements personnels le concernant et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes.

La Loi confère au Commissaire à la protection de la vie privée du Canada le rôle d'ombudsman lorsque des plaintes sont déposées aux termes des nouvelles dispositions législatives. Dans la mesure du possible, le Commissaire s'efforce de régler les problèmes au moyen du respect volontaire plutôt que de l'exécution stricte de la Loi. Il instruit les plaintes, effectue des vérifications, sensibilise les intéressés aux questions relatives à la protection des renseignements personnels et mène des recherches à ce sujet. Il fait également office d'ombudsman lorsque des plaintes sont déposées aux termes de la *Loi sur la protection des renseignements personnels*, qui vise le secteur public fédéral.

La Partie 1 de la Loi entrera en vigueur en trois étapes, à compter du 1er janvier 2001.

Pour plus de renseignements, communiquez avec :

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

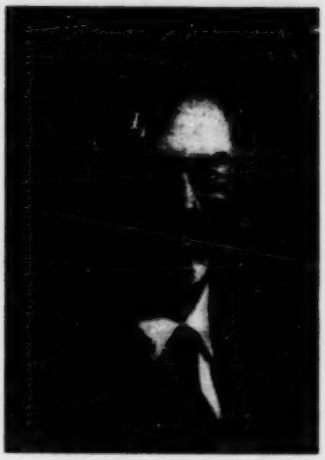
Téléphone : 1-613-995-8210
Sans frais : 1-800-282-1376
Télécopieur : 1-613-947-6850
Site Web : www.privcom.gc.ca
Courriel : info@privcom.gc.ca

Même si on a tout mis en oeuvre pour qu'il soit exact et exhaustif, le présent guide n'a pas de statut juridique. Pour obtenir le texte officiel de la nouvelle Loi, consultez notre site Web à www.privcom.gc.ca ou téléphonez au bureau du Commissaire à la protection de la vie privée.

This publication is also available in English.

* Le présent guide ne porte que sur la Partie 1 de la Loi. Les renvois à la Loi dans le présent document ne concernent que la Partie1. Les parties 2 à 5 de la Loi ont trait à l'utilisation des signatures et des documents électroniques comme solutions de rechange licites aux signatures et aux documents originaux. Pour obtenir plus de renseignements à ce sujet, communiquez avec le ministère de la Justice.

Du Commissaire à la protection de la vie privée du Canada



L'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* est un pas en avant non négligeable pour le Canada. Elle le propulse au premier plan des nations qui profitent des progrès de la technologie et du commerce électronique, sans négliger pour autant de protéger et même d'accroître des droits fondamentaux qui lui sont chers depuis longtemps.

Nous savons tous que les Canadiens même s'ils se préoccupent de la protection de la vie privée, ou s'enthousiasment pour la nouvelle économie, restent prudents au sujet des renseignements personnels qui les concernent. Mais les entreprises, en revanche, pourront voir quelque chose d'inédit dans le fait qu'elles peuvent tirer avantage du respect des pratiques équitables de traitement de l'information et des principes de protection de la vie privée énoncés dans la *Loi sur la protection des renseignements personnels et les documents électroniques*. Cette Loi porte en fait sur de saines pratiques de gestion de l'information, dont toute organisation peut tirer profit. Nous avons rédigé ce guide pour aider les entreprises à mesurer ce que cette nouvelle Loi exige d'elles, et leur permettre de bénéficier pleinement de l'adoption des pratiques équitables de traitement de l'information qui sont au cœur même de la Loi.

La Loi n'est pas toujours simple et directe - c'est un texte de loi après tout - bien que les principes qu'elle énonce soient assez clairs. Le *Code type sur la protection des renseignements personnels*, de l'Association canadienne de normalisation, qui a été élaboré par des entreprises au moyen d'un processus de consultation, est intégré dans la Loi sous forme d'appendice (ce que les rédacteurs juridiques appellent une annexe). Pour lire ce texte législatif, il faut donc faire des allers et retours pour passer de la loi au Code. Je crois que la Loi est le reflet du processus ayant conduit à sa création, qui résulte de la difficile atteinte d'un consensus entre entrepreneurs, protecteurs des consommateurs et experts des politiques gouvernementales. Je pense aussi que les entreprises perceveront tout inconvénient dû à la structure de la loi comme un faible prix à payer pour obtenir une réglementation qui tient compte de leurs commentaires, de leurs besoins et de leurs diverses pratiques commerciales. J'ai bon espoir que pour la plupart des entreprises l'application de cette Loi sera vécue davantage comme une autoréglementation et non comme une réglementation gouvernementale. Je le répète, les principes et pratiques que renferme cette loi sont faciles à saisir : ce sont de bonnnes habitudes d'affaires, pleines de bon sens.

À la lecture du guide, vous constaterez le rôle qu'a joué mon bureau, c'est-à-dire d'abord celui d'ombudsman de la protection de la vie privée, déterminé à aller au fond des choses et à trouver des solutions qui conviennent à toutes les parties. Je prends ce rôle très au sérieux, et je vous assure que notre fonction de surveillance vise aussi à offrir de l'aide et des conseils aux entreprises à la recherche de meilleurs moyens d'assurer la protection de la vie privée. Je serai heureux d'entretenir avec les entreprises des relations marquées au coin du dynamisme et du respect pour mieux entrer dans cette nouvelle ère de la protection de la vie privée. Nous avons tous un défi à relever, beaucoup de choses à apprendre - et beaucoup à gagner.

Un grand nombre de personnes ont consacré bien des mois à la réalisation de ce guide. Je veux exprimer toute ma reconnaissance aux nombreuses organisations du secteur privé qui ont bien voulu examiner ce document à divers stades de son élaboration. Sachez que vos conseils et vos commentaires ont toujours été réfléchis et pratiques.

Je suis impatient de poursuivre cette collaboration en vue de travailler avec vous, au cours des mois et des années à venir, à la protection de la vie privée des Canadiens et des Canadiennes.

George Radwanski
Commissaire à la protection de la vie privée du Canada

Table des matières

- **La Loi en bref**
- **Votre organisation est-elle visée par la Loi?**
- **Quelles sont les exclusions?**
- **Les responsabilités imposées par la Loi**
  1. **Responsabilité**
  2. **Détermination des fins de la collecte de renseignements**
  3. **Consentement**
  4. **Limite de la collecte**
  5. **Limitation de l'utilisation, de la communication et de la conservation**
  6. **Exactitude**
  7. **Mesures de sécurité**
  8. **Transparence**
  9. **Accès aux renseignements personnels**
  10. **Dépôt de plaintes**
- **Exceptions aux principes du consentement et de l'accès**
- **Rôle du Commissaire à la protection de la vie privée**
- **Plaintes devant le Commissaire à la protection de la vie privée**
- **Recours devant la Cour fédérale**
- **Vérifications des pratiques de gestion des renseignements personnels**
- **Questionnaire sur la protection des renseignements personnels**

La Loi en bref

▲

Les organisations visées par la Loi doivent obtenir le consentement de l'intéressé lorsqu'elles recueillent, utilisent ou communiquent des renseignements personnels le concernant. L'intéressé a le droit de consulter les renseignements personnels que détient une organisation à son sujet et, au besoin, d'en contester l'exactitude. Les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis. L'organisation qui entend les utiliser à une autre fin doit obtenir un nouveau consentement. Les particuliers devraient également avoir l'assurance que les renseignements qui les concernent seront protégés au moyen de mesures de sécurité précises, notamment des classeurs verrouillés, des mots de passe informatiques ou le chiffrement.

Renseignements personnels

Par « renseignements personnels », on entend tout renseignement factuel ou subjectif, consigné ou non, concernant un individu identifiable. Il peut s'agir de tout type de renseignements, notamment :

- l'âge, le nom, les numéros d'immatriculation, le revenu, l'origine ethnique ou le type sanguin;
- des opinions, des évaluations, des commentaires, le statut social ou les mesures disciplinaires;
- les dossiers d'employé, les dossiers de crédit, les dossiers relatifs à des prêts, les dossiers médicaux, l'existence d'un différend entre un consommateur et un marchand, des intentions (p. ex., d'acquérir des biens ou des services ou de changer d'emploi).

Les renseignements personnels ne comprennent pas le nom, le titre ni l'adresse ou le numéro de téléphone au travail d'un employé d'une organisation.

Plaintes

En cas de violation alléguée de la Loi, l'on peut déposer une plainte auprès de l'organisation en question ou du Commissaire à la protection de la vie privée. Le Commissaire peut lui-même prendre l'initiative d'une plainte.

Requête devant la Cour fédérale

Après avoir reçu le rapport d'enquête du Commissaire, le plaignant peut demander à la Cour fédérale de l'entendre, à certaines conditions énoncées dans l'article 14 de la Loi. Le Commissaire à la protection de la vie privée peut également, au nom du plaignant ou en son nom propre, demander à être entendu par la Cour. Cette dernière peut ordonner à une organisation de modifier ses pratiques ou d'accorder au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie.

Vérifications

Le Commissaire peut, avec un préavis suffisant, procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels.

Dénonciation

Toute personne qui estime que les articles 5 à 10 de la Loi ont été violés ou sont sur le point de l'être peut prévenir le Commissaire et exiger que son identité soit tenue confidentielle. Une fois qu'il a donné cette assurance, le Commissaire est tenu de protéger l'anonymat du dénonciateur.

Infraction

Commet une infraction quiconque :

- détruit des renseignements personnels demandés par un particulier;
- use de représailles contre un employé qui a déposé une plainte auprès du Commissaire ou qui refuse de contrevenir aux articles 5 à 10 de la Loi;
- nuit à l'instruction d'une plainte ou à la conduite d'une vérification menée par le Commissaire ou son délégué.

Le contrevenant est passible, par procédure sommaire, d'une amende maximale de 10 000 $ et, par mise en accusation, d'une amende maximale de 100 000 $.

Définitions

Entreprises fédérales

Sont comprises les « installations, ouvrages, entreprises ou secteurs d"activités qui relèvent de la compétence législative du Parlement ». Même si la plupart des organisations réglementées par le gouvernement fédéral sont visées par la définition, tous les types d'organisations ne sont pas des entreprises fédérales. Par exemple, les compagnies d'assurances et les coopératives de crédit ont beau être visées par certains règlements fédéraux, elles n'en relèvent pas moins de la compétence des provinces aux termes de la Constitution. À ce titre, elles ne sont pas considérées comme des entreprises fédérales aux fins de la Loi. Dans cette dernière, on définit certains types d'entreprises visées par la Partie I :

- le transport inter-provincial ou international par voie terrestre ou par eau;
- les aéroports, les aéronefs ou les lignes de transport aérien;
- les télécommunications;
- les stations de radiodiffusion et de télédiffusion;
- les banques;
- les élévateurs à grain;
- les centrales nucléaires;
- les entreprises de forage en mer.

Il convient de noter qu'il ne s'agit pas ici d'une liste exhaustive des « entreprises fédérales ». Votre entreprise ne constitue pas une « entreprise fédérale » du seul fait qu'elle est constituée sous le régime de la loi fédérale. Si elle visée par l'une ou l'autre des parties du *Code canadien du travail*, votre société est probablement une « entreprise fédérale ».

Activité commerciale

Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds.

Organisation

S'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales.

Consentement

Acceptation volontaire de ce qui est fait ou proposé. Le consentement peut être explicite ou implicite. Le consentement explicite est expressément donné, verbalement ou par écrit. Sans équivoque, le consentement explicite ne suppose aucune inférence de la part de l'organisation qui cherche à obtenir le consentement. Il y a consentement implicite lorsque le comportement ou l'inaction de l'intéressé permet raisonnablement de conclure au consentement.

Communication

Rendre des renseignements personnels accessibles à des personnes de l'extérieur de l'organisation.

Utilisation

Désigne le traitement des renseignements personnels au sein d'une organisation.

Votre organisation est-elle visée par la Loi?

La Loi s'appliquera aux organisations en trois étapes :

Le 1er janvier 2001

Dans un premier temps, la Loi s'applique aux renseignements personnels (à l'exception des renseignements personnels sur la santé) recueillis, utilisés ou communiqués dans le cadre des activités commerciales d'entreprises fédérales. La liste comprend notamment les organisations réglementées par le gouvernement fédéral comme les banques, les sociétés de télécommunications et les entreprises de transport.

À ce stade, la Loi s'applique également aux renseignements personnels recueillis, utilisés ou communiqués par les mêmes organisations au sujet de leurs employés.

En outre, la Loi s'applique à la communication de renseignements personnels moyennant contrepartie au-delà des frontières provinciales ou nationales par des organisations comme les agences d'évaluation du crédit ou des organisations qui louent, vendent ou échangent des listes d'abonnés ou d'autres renseignements personnels. Les renseignements doivent être eux-mêmes l'objet de la transaction, et la contrepartie doit être accordée pour les renseignements.

Le 1er janvier 2002

Pour les organisations et les activités visées à la première étape, la Loi s'applique aux renseignements personnels sur la santé. « Renseignement personnel sur la santé » s'entend de tout renseignement ayant trait à la santé mentale ou physique, y compris les services de santé fournis de même que les résultats de tests et d'examens.

Le 1er janvier 2004

La Loi s'applique à la collecte, à l'utilisation ou à la communication de renseignements personnels dans le cadre de toute activité commerciale au sein d'une province. Cependant, le gouvernement peut exclure des organisations ou des activités dans les provinces qui ont, dans le domaine de la protection des renseignements personnels, adopté une loi essentiellement similaire.

La Loi s'appliquera également à tout renseignement personnel touchant l'ensemble des transactions interprovinciales et internationales réalisées par l'ensemble des organisations visées par la Loi dans le cadre de leurs activités commerciales.

Le Québec est la seule province aujourd'hui dotée de dispositions législatives concernant les renseignements personnels dans le secteur privé. Le gouvernement fédéral a affirmé que la loi québécoise répondait au critère défini par la notion d'«essentiellement similaire», et que les organisations et les activités visées par la loi québécoise seront exclues de la loi fédérale en ce qui a trait aux questions intraprovinciales.

D'autres provinces et territoires envisagent l'adoption de dispositions législatives applicables au secteur privé.

Test rapide

Votre organisation est-elle une entreprise fédérale qui recueille, utilise ou communique des renseignements personnels dans le cadre d'une activité commerciale?

Si la réponse est OUI, elle sera visée par la Loi à compter du 1er janvier 2001. La Loi s'appliquera aux renseignements personnels concernant vos employés aussi bien que vos clients.

Si la réponse est NON :
Communiquez-vous des renseignements personnels pour contrepartie à l'extérieur de la province? En d'autres termes, les renseignements personnels sont-ils l'objet de la transaction?

Si la réponse est OUI, la communication est visée par la Loi à compter du 1er janvier 2001.

Quelles sont les exclusions?

- La collecte, l'utilisation ou la communication de renseignements personnels par des institutions fédérales auxquelles s'applique la *Loi sur la protection des renseignements personnels*.
- Les gouvernements provinciaux et territoriaux et leurs mandataires.
- Le nom, le titre, l'adresse ou le numéro de téléphone au travail d'un employé.
- La cueillette, l'utilisation ou la communication de renseignements personnels par un particulier à des fins strictement personnelles (p. ex., la constitution d'une liste de personnes à qui adresser des cartes de voeux).
- La cueillette, l'utilisation et la communication de renseignements personnels par une organisation à des fins strictement journalistiques, artistiques ou littéraires.

Les responsabilités imposées par la Loi

Les organisations du secteur privé doivent respecter un code sur la protection des renseignements personnels, lequel constitue l'Annexe 1 de la Loi.

Le code a été élaboré par des entreprises, des consommateurs, des chercheurs et le gouvernement sous les auspices de l'Association canadienne de normalisation. On y énonce dix principes concernant les pratiques équitables de traitement des renseignements, qui servent de règles de base à la cueillette, à l'utilisation et à la communication de renseignements personnels. Ces principes permettent aux intéressés d'exercer une mainmise sur la façon dont le secteur privé traite les renseignements personnels les concernant.

Une organisation est responsable des renseignements personnels dont elle a la gestion et doit traiter ceux-ci de façon équitable en tout temps, à l'intérieur de ses cadres aussi bien que dans ses tractations avec des tierces parties. La prudence dans la collecte, l'utilisation et la communication des renseignements personnels représente un élément essentiel pour assurer la confiance et la fidélité des consommateurs.

Voici la liste des dix principes que les entreprises doivent respecter :

1. la responsabilité
2. la détermination des fins de la collecte des renseignements;
3. le consentement;
4. la limitation de la collecte;
5. la limitation de l'utilisation, de la communication et de la conservation;
6. l'exactitude;
7. les mesures de sécurité;
8. la transparence;
9. l'accès aux renseignements personnels;
10. la possibilité de porter de porter plainte à l'égard du non-respect des principes.

Ces principes doivent être interprétés conjointement avec les principales sections de la Loi, en particulier :

Les articles 2 à 10 de la Loi

On doit interpréter l'Annexe 1 conjointement avec les articles 2 à 10 de la Loi. Il est essentiel d'étudier avec soin les obligations définies dans ces sections, parallèlement aux dix principes.

Article 2

- Fournit des définitions, notamment d'activité commerciale, d'entreprises fédérales, de renseignements personnels, de renseignements personnels sur la santé et d'organisation.
- Précise que les notes afférentes des articles 4.3 et 4.9 de l'Annexe 1 ne font pas partie de la Loi.

Article 3

Définit l'objet de la Loi :

- reconnaître le droit des particuliers à la protection des renseignements personnels les concernant;
- reconnaître le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes;
- établir des règles relatives au traitement des renseignements personnels.

Article 4

Définit le champ d'application de la Loi :

- toutes les organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales;
- les renseignements personnels concernant un employé d'une entreprise fédérale, mais non les renseignements personnels du secteur privé.

Article 5

- Précise que toute organisation doit se conformer aux obligations énoncées dans l'Annexe 1.
- Précise ce qui est exclu de la Loi.
- Dans l'Annexe :
  - Le verbe « doit » s'entend d'une obligation.
  - Le conditionnel (par exemple) « devrait » signifie qu'il s'agit d'une recommandation et non d'une obligation.
- Limite la cueillette, l'utilisation ou la communication des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Dans l'application de toute disposition de la Partie 1 de la Loi, on doit tenir compte de la notion de «personne raisonnable».

Article 6

- Précise que le fait de confier à une personne la responsabilité de la conformité n'exempte pas l'organisation des obligations énoncées à l'Annexe 1.

Article 7

- Précise dans quelles circonstances les renseignements personnels peuvent être recueillis, utilisés ou communiqués sans le consentement de l'intéressé.

Article 8

- Définit les démarches que doivent effectuer les intéressés qui souhaitent présenter une demande de communication relative à des renseignements personnels ou apporter des corrections à des renseignements personnels les concernant.

Article 9

- Explique les circonstances dans lesquelles l'accès à des renseignements personnels peut être refusé.

Article 10

- Précise l'obligation qu'a une organisation de fournir les renseignements personnels sur support de substitution (p. ex., braille, gros caractères ou bande audio) à toute personne ayant une déficience sensorielle.

Principes relatifs à l'équité dans le traitement des renseignements

- Dans la partie qui suit, on énonce les responsabilités applicables à chacun des dix principes relatifs à l'équité dans le traitement des renseignements personnels définis à l'Annexe 1. Vous y trouverez des conseils et des moyens de vous acquitter de vos responsabilités.

La personne raisonnable

L'article 5 de la Loi limite la collecte, l'utilisation et la communication des renseignements personnels à des fins qu'une «personne raisonnable» estimerait acceptables dans les circonstances. Voici des exemples :

- Un client qui loue un film dans un club vidéo estimera-t-il acceptable qu'on l'oblige à donner son numéro de téléphone? Son adresse? Son numéro d'assurance sociale?
- Un client qui paie comptant pour un produit ou un service estimera-t-il raisonnable qu'on lui demande son nom, son adresse et son numéro de téléphone?

1. Responsabilité

Vos responsabilités

- Respecter les dix principes énoncés à l'Annexe 1.
- Confier à une personne (ou à des personnes) la responsabilité du respect de la Loi par votre organisation.
- Protéger tous les renseignements personnels que votre entreprise a en sa possession, y compris les renseignements confiés à une tierce partie aux fins de traitement.
- Élaborer et mettre en œuvre des politiques et des pratiques concernant les renseignements personnels.

Comment vous acquitter de vos responsabilités

- Donnez au responsable de la protection des renseignements personnels le soutien de la haute direction et les pouvoirs voulus pour intervenir dans toute question concernant la protection des renseignements personnels qui ont un rapport avec les activités de votre organisation.
- Communiquez le nom ou le titre de la personne en question à l'interne et à l'externe (p. ex. dans les sites Web et les publications).
- Assurez-vous que l'ensemble des pratiques relatives au traitement des renseignements personnels, y compris les activités en cours et les nouvelles initiatives, sont équitables, à l'aide de la liste de contrôle qui suit :

  - quels renseignements personnels recueillons-nous?
  - pourquoi les recueillons-nous?
  - comment les recueillons-nous?
  - à quelles fins les utilisons-nous?
  - où les conservons-nous?
  - dans quelle mesure sont-ils en sécurité?
  - qui y a accès ou les utilise?
  - à qui sont-ils communiqués?
  - quand sont-ils éliminés?

- Élaborez et mettez en œuvre des politiques et des procédures pour assurer la protection des renseignements personnels:

  - précisez les fins auxquelles ils sont recueillis;
  - obtenez le consentement des intéressés;
  - limitez la collecte, l'utilisation et la communication des renseignements personnels;
  - assurez-vous que les renseignements sont exacts, complets et à jour;
  - prenez des mesures de sécurité suffisantes;
  - élaborez ou mettez à jour un calendrier pour la conservation et la destruction des documents
  - traitez les demandes de communication;
  - donnez suite aux demandes de renseignements et aux plaintes.

- Assortissez les contrats d'une disposition relative à la protection des renseignements personnels pour vous assurer que la tierce partie prend des mesures de sécurité comparables aux vôtres.
- Informez vos employés des politiques et procédures concernant la protection des renseignements personnels et assurez-leur la formation voulue.
- Mettez à la disposition des clients et des clients de l'information sur ces politiques et procédures (p. ex. dépliants et sites Web).

Conseils

Formez vos employés de première ligne et vos cadres et tenez-les au courant, de façon qu'ils puissent répondre aux questions suivantes :

- Comment donner suite aux demandes de renseignements du public au sujet des politiques de l'organisation concernant la protection des renseignements personnels?
- Qu'est-ce que le consentement? Quand et comment doit-on l'obtenir?
- Comment reconnaître et traiter les demandes de communication de renseignements personnels?
- À qui devrais-je transmettre les plaintes concernant des questions liées à la protection des renseignements personnels?
- Quels sont les droits et les garanties dont je bénéficie en ce qui a trait à la protection des renseignements personnels? (La question s'applique aux employés des organisations réglementées par le gouvernement fédéral.)
- Quelles sont les activités courantes et les nouvelles initiatives menées dans notre organisation dans le domaine de la protection des renseignements personnels?

Avant de transmettre des renseignements personnels à des tierces parties, prenez les précautions suivantes :

- Désignez une personne chargée de traiter de tous les aspects du contrat liés à la protection des renseignements personnels;
- Limitez l'utilisation des renseignements personnels aux fins nécessaires à l'exécution du contrat;
- Limitez la communication des renseignements à ce qui est autorisé par votre organisation ou prescrit par la Loi;
- Aiguillez vers votre organisation les personnes qui souhaitent consulter les renseignements personnels les concernant;
- À la fin du contrat, retournez les renseignements transmis ou détruisez-les;
- Utilisez les mesures de sécurité qui s'imposent pour assurer la protection des renseignements personnels;
- Au besoin, donnez à votre organisation la possibilité de vérifier la mesure dans laquelle la tierce partie respecte les dispositions du contrat.

2. Détermination des fins de la collecte des renseignements

▲

Il revient à votre organisation de préciser les motifs de la collecte de renseignements personnels, avant ou pendant celle-ci.

Vos responsabilités

- Avant ou pendant toute collecte de renseignements personnels, préciser pourquoi les renseignements sont nécessaires et comment ils seront utilisés.
- Documenter les fins auxquelles les renseignements sont recueillis.
- Préciser à la personne auprès de qui on recueille des renseignements les fins auxquelles ceux-ci sont destinés.
- Définir toute nouvelle fin à laquelle les renseignements sont destinés, et obtenir le consentement de l'intéressé avant de les utiliser.

Comment vous acquitter de vos responsabilités

- Examinez les renseignements personnels que vous avez en votre possession pour déterminer s'ils sont tous destinés à une fin précise.
- Informez le particulier, verbalement ou par écrit, des fins auxquelles les renseignements sont destinés.
- Consignez par écrit toutes les fins définies et obtenez les consentements voulus de façon à pouvoir vous y référer facilement au cas où on vous demanderait de rendre des comptes à ce sujet.

Assurez-vous que les fins auxquelles les renseignements sont destinés se limitent à ce qu'une personne raisonnable estimerait acceptable dans les circonstances.

Conseils

- Définissez le plus clairement et le plus étroitement possible à quelles fins les données sont recueillies, de façon que l'intéressé comprenne comment ils seront utilisés ou communiqués.
- Évitez les fins trop vastes, qui risquent d'aller à l'encontre du principe de la connaissance et du consentement.
- Voici quelques exemples de fins :

  - ouvrir un compte;
  - vérifier la solvabilité;
  - assurer des avantages aux employés;
  - traiter une demande d'abonnement à un magazine;
  - poster de l'information au sujet de l'adhésion à une association;
  - garantir une réservation de voyage;
  - établir les préférences d'un client;
  - définir l'admissibilité d'un client à un rabais ou à une offre spéciale.

3. Consentement

▲

Vos responsabilités

- Bien informer l'intéressé des fins de la collecte, de l'utilisation ou de la communication des renseignements personnels.
- Obtenir le consentement de l'intéressé avant ou pendant la collecte des renseignements de même qu'au moment d'une nouvelle utilisation.

Comment vous acquitter de vos responsabilités

- Obtenez le consentement de la personne à propos de qui des renseignements personnels sont recueillis, utilisés ou communiqués.
- Communiquez de façon claire et raisonnablement intelligible.
- Consignez par écrit le consentement reçu (p. ex. conservez dans le dossier une note ou encore une copie du message

électronique ou du document dans lequel l'intéressé a coché la case appropriée).

- N'obtenez jamais de consentement par des moyens détournés.
- Ne faites pas de l'obtention du consentement une condition de la fourniture d'un produit ou d'un service, à moins que le renseignement requis ne s'impose à des fins explicites et légitimes.
- Expliquez aux particuliers les conséquences du retrait de leur consentement.
- Veillez à ce que les employés qui recueillent des renseignements personnels soient en mesure de répondre aux questions de l'intéressé au sujet des fins auxquelles les renseignements sont recueillis.

Conseils

- On obtient normalement le consentement de la personne à propos de qui des renseignements personnels sont recueillis, utilisés ou communiqués.
- On peut obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale auprès du tuteur ou du détenteur d'une procuration.
- Le consentement n'est valable que si les intéressés comprennent à quelles fins les renseignements qui les concernent seront utilisés.
- Les consentements devraient :

  - être faciles à trouver;
  - être rédigés de façon claire et directe;
  - ne pas s'appuyer sur des catégories générales de fins, d'utilisations et de communications;
  - préciser le mieux possible quelles organisations traitent les renseignements.

- Le consentement peut être obtenu en personne, par téléphone, par la poste, par Internet, etc.
- Au moment d'établir la forme du consentement, on devrait tenir compte des éléments suivants :

  - les attentes raisonnables de l'intéressé;
  - les circonstances entourant la cueillette;
  - le caractère délicat des renseignements en question.

- Dans la mesure du possible, on devrait obtenir un consentement explicite. Lorsqu'il s'agit de renseignements considérés comme délicats, on doit toujours obtenir un tel consentement. L'obtention d'un consentement explicite protège l'intéressé comme l'organisation.

- Il y a certaines exceptions au principe du consentement.

Droits acquis

Les renseignements personnels que votre société a recueillis dans le cadre de ses activités commerciales sont visés par la Loi. Comme les renseignements en question ont déjà été recueillis, vous n'avez pas à les recueillir de nouveau. Afin de pouvoir continuer de les utiliser ou de les communiquer, la Loi vous oblige maintenant à obtenir un consentement. Certaines organisations ont informé l'ensemble de leurs clients de l'utilisation qu'elles font des renseignements qui les concernent et des institutions auxquelles ils sont communiqués, tout en donnant à ces derniers la possibilité de s'opposer à ces utilisations ou communications systématiques.

4. Limite de la collecte

Vos responsabilités

- Ne pas recueillir de renseignements personnels à tort et à travers.
- Ne pas tromper ni induire en erreur des particuliers à propos des motifs de la cueillette de renseignements personnels.

Comment vous acquitter de vos responsabilités

- Limitez la quantité et le type de renseignements recueillis à ce qu'exigent les fins définies.
- Définissez le genre de renseignements personnels que vous recueillez dans vos politiques et pratiques relatives au traitement des renseignements.
- Assurez-vous que les membres de votre personnel sont en mesure d'expliquer les motifs de la collecte de renseignements.

Conseils

- En réduisant la quantité de renseignements recueillis, vous pouvez réduire les coûts de la collecte, de l'emmagasinage, de la conservation et, en dernière analyse, de l'archivage des données.
- Le fait de recueillir moins de renseignements entraîne également une réduction des risques d'utilisation et de communications impropres.

5. Limitation de l'utilisation, de la communication et de la conservation

Vos responsabilités

- N'utiliser ou ne communiquer les renseignements personnels qu'aux fins auxquelles ils ont été recueillis, à moins que l'intéressé ne donne son consentement ou que l'utilisation ou la communication ne soit autorisée par la Loi.
- Ne garder les renseignements personnels que le temps de satisfaire aux fins voulues.
- Établir des lignes directrices et des procédures relatives à la conservation et à la destruction des renseignements personnels.
- Conserver les renseignements personnels utilisés pour prendre une décision au sujet d'une personne pendant un temps raisonnable. Celle-ci devrait ainsi pouvoir obtenir les renseignements une fois la décision prise et, le cas échéant, exercer un recours.
- Détruire, effacer ou rendre anonymes les renseignements qui ne sont plus nécessaires à une fin donnée ou prescrite par la Loi.

Comment vous acquitter de vos responsabilités

- Documentez toute nouvelle fin relative à l'utilisation des renseignements personnels.
- Établissez des périodes de conservation maximales et minimales qui tiennent compte des exigences ou des restrictions législatives ainsi que des mécanismes de redressement.
- Supprimez les renseignements qui ne répondent pas à une fin précise ou qui ne satisfont plus à la fin voulue.
- Détruisez les renseignements personnels de manière à prévenir les possibilités d'accès illicites.
- Détruisez les renseignements personnels de manière à prévenir l'accès à ceux-ci. La solution idéale consiste à déchiqueter les dossiers sur support papier et à effacer les fichiers sur support électronique.
- Établissez des politiques définissant les types de renseignements qui doivent être mis à jour. Une organisation peut raisonnablement s'attendre à ce qu'une personne fournisse des renseignements à jour dans certaines circonstances (p. ex., un changement d'adresse dans le cas d'un abonnement à un magazine).

Conseils

- Il est parfois moins coûteux et compliqué de détruire ou d'effacer des renseignements que de les rendre anonymes.
- Procéder à des examens périodiques pour déterminer si des renseignements sont toujours nécessaires. Pour se faciliter la tâche, on peut établir un calendrier de conservation.

6. Exactitude

▲

Vos responsabilités

Réduire au minimum les possibilités d'utilisation impropres des renseignements personnels au moment de prendre une décision concernant l'intéressé ou de communiquer les renseignements à des tierces parties.

Comment vous acquitter de vos responsabilités

- Veillez à ce que les renseignements soient aussi exacts, complets et à jour que nécessaire, compte tenu de leur utilisation et des intérêts de l'intéressé.
- Ne mettez les renseignements à jour que si les fins auxquelles ils sont destinés l'exigent.
- Veillez à ce que les renseignements fréquemment utilisés soient exacts et à jour, à moins que des limites claires ne soient prévues à ces égards.

Conseils

- Déterminer si l'utilisation et la communication de renseignements désuets ou incomplets porteraient préjudice à l'intéressé constitue une façon de déterminer si les renseignements doivent être actualisés.
- Pour assurer l'exactitude, vous pouvez utiliser la liste de contrôle suivante :

  - énumérez le type de renseignements personnels nécessaires à la prestation d'un service;
  - repérez la banque où tous les renseignements personnels connexes peuvent être récupérés;
  - consignez par écrit la date à laquelle les renseignements personnels ont été récupérés ou mis à jour;
  - consignez par écrit les mesures prises pour vérifier l'exactitude, l'exhaustivité et l'à-propos des renseignements.

  Pour ce faire, vous devrez peut-être passer vos dossiers en revue ou communiquer avec le client.

7. Mesures de sécurité

▲

Vos responsabilités

- Protéger les renseignements personnels contre la perte ou le vol.
- Protéger les renseignements contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.
- Protéger les renseignements personnels, quelle que soit la forme sous laquelle ils sont conservés.

Comment vous acquitter de vos responsabilités

- Élaborez et appliquez une politique de sécurité pour assurer la protection des renseignements personnels.
- Utilisez des mesures de sécurité adéquates pour assurer la protection qui s'impose :

  - des moyens matériels (le verrouillage des classeurs, la restriction de l'accès aux bureaux, des systèmes d'alarme);
  - des outils technologiques (des mots de passe, le chiffrement, des coupe-feu, des logiciels servant à préserver l'anonymat des intéressés);
  - des mesures administratives (des autorisations sécuritaires, l'accès sélectif, la formation des employés, des ententes de non-divulgation).

- Assurez-vous que les employés sont conscients de l'importance que revêtent la sécurité et la confidentialité des renseignements personnels.
- Sensibilisez les employés aux mesures de sécurité en organisant périodiquement des réunions à ce sujet.
- Au moment de choisir les mesures de sécurité qui s'imposent, il conviendrait de tenir compte des facteurs suivants :

  - le caractère délicat des renseignements;
  - la quantité de renseignements;
  - l'importance de leur distribution;
  - leur présentation (support électronique, support papier, etc.);
  - le type d'emmagasinage.

- Examinez et mettez à jour les mesures de sécurité de façon périodique.

Conseils

- Au moment de fournir des copies des renseignements à des tiers, assurez-vous que les renseignements personnels qui n'ont rien à avoir avec la transaction sont supprimés ou masqués.
- Conservez les dossiers qui renferment des renseignements délicats dans un lieu ou dans un système informatique sûr et assurez-vous que l'accès à ces renseignements est limité aux personnes autorisées.

8. Transparence

Vos responsabilités

- Informer les clients et les employés des politiques et des pratiques de gestion des renseignements personnels en vigueur.
- Faire en sorte que ces politiques et pratiques soient compréhensibles et faciles d'accès.

Comment vous acquitter de vos responsabilités

- Veillez à ce que les employés de première ligne soient au fait des procédures afin de pouvoir répondre aux demandes de renseignements d'un particulier.
- Rendez publiques les informations suivantes :

  - le nom ou le titre et l'adresse de la personne responsable des politiques et des pratiques de protection des renseignements personnels de votre organisation;
  - le nom ou le titre et l'adresse de la personne à qui les demandes de communication devraient être

expédiées;
- la marche à suivre par les particuliers pour consulter les renseignements personnels les concernant;
- la marche à suivre en vue du dépôt d'une plainte auprès de votre organisation;
- des dépliants ou d'autres renseignements expliquant les politiques, les normes ou les codes de votre organisation;
- une description des renseignements personnels mis à la disposition d'autres organisations (y compris les filiales) et des motifs de la communication de ces renseignements.

Conseil

- L'information concernant vos politiques et pratiques peut être accessible en personne, par écrit, par téléphone, dans des publications ou dans le site Web de votre organisation.

9. Accès aux renseignements personnels

▲

Vos responsabilités

- Informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent.
- Expliquer l'usage qui en est fait ou qui en a été fait et fournir une liste de toutes les organisations auxquelles les renseignements ont été communiqués.
- Donner aux particuliers la possibilité de consulter les renseignements qui les concernent.
- Corriger ou modifier les renseignements personnels si leur exactitude et leur exhaustivité sont contestées et se révèlent effectivement déficientes.
- Fournir une copie des renseignements demandés ou des motifs pour lesquels l'accès est refusé, sous réserve des exceptions définies à l'article 9 de la Loi (voir ci-après).
- Une organisation devrait consigner tous les désaccords au sujet du dossier et, le cas échéant, informer les tierces parties.

Comment vous acquitter de vos responsabilités

▲

- Le cas échéant, aidez le particulier à préparer une demande de consultation des renseignements personnels le concernant.
- Vous pouvez demander au particulier de fournir suffisamment de renseignements pour qu'il vous soit possible de le renseigner sur l'existence, l'utilisation et la communication de renseignements personnels.
- Donnez suite à la demande le plus rapidement possible et, au plus tard, 30 jours suivant sa réception.
- Le délai habituel de traitement peut être prolongé d'une période maximale de 30 jours, selon les critères définis au paragraphe 8(4) de la Loi :

  - l'observation du délai initial de 30 jours entraverait gravement l'activité de l'organisation;
  - vous avez besoin de plus de temps pour mener des consultations;
  - vous avez besoin de temps pour transférer les renseignements personnels sur un support de substitution.

- Si votre organisation choisit de se prévaloir d'une prorogation de délai, vous devez informer l'auteur de la demande dans les 30 jours suivant la réception de cette dernière ainsi que de son droit de porter plainte auprès du Commissaire à la protection de la vie privée.
- Assurez au particulier un accès gratuit ou à prix modique aux renseignements.
- Informez le particulier des coûts approximatifs avant de traiter la demande.
- Permettez au particulier de consulter les renseignements personnels qui les concernent.
- Veillez à ce que les renseignements demandés soient compréhensibles. Expliquez les acronymes, les abréviations et les codes.
- Le cas échéant, transmettez les renseignements modifiés aux tierces parties qui y ont accès.

- Informez par écrit le particulier dont la demande de communication est refusée et énoncez les motifs de la décision et les recours.
- Le principe de l'accès aux renseignements personnels est assujetti à des exceptions.

Conseils

- Conservez en un seul lieu les renseignements personnels concernant des particuliers afin d'en faciliter l'extraction. Sinon, consignez par écrit tous les endroits où se trouvent de tels renseignements.
- Ne communiquez les renseignements personnels que lorsque vous êtes certain de l'identité de l'auteur de la demande et du droit d'accès de ce dernier.
- Si vous ne stockez pas tous les renseignements personnels au même endroit, consignez dans un registre les endroits où ils le sont afin d'en faciliter l'extraction.

10. Dépôt de plaintes

Vos responsabilités

- Élaborer des procédures simples et faciles d'accès pour le dépôt des plaintes.
- Informer les plaignants des recours qui s'offrent à eux, notamment les procédures d'instruction des plaintes de votre organisation, celles des associations industrielles, des organismes de réglementation et du Commissaire à la protection de la vie privée du Canada.
- Instruire toutes les plaintes reçues.
- Prendre les mesures qui s'imposent pour corriger les pratiques et les politiques de traitement des renseignements.

Comment vous acquitter de vos responsabilités

- Consignez la date de réception de la plainte et la nature de cette dernière (par exemple, retard dans le traitement d'une demande, réponse incomplète ou inexacte ou encore collecte, utilisation, communication ou conservation inadéquates).
- Accusez réception de la plainte sans délai.
- Au besoin, communiquez avec l'intéressé pour clarifier la plainte.
- Confiez l'enquête à une personne possédant les compétences voulues pour mener celle-ci avec équité et impartialité.
- Permettez à l'enquêteur de consulter tous les dossiers, les employés ou les autres intervenants qui ont traité les renseignements personnels ou la demande de communication.
- Informez clairement et rapidement l'intéressé du résultat de l'enquête ainsi que des mesures pertinentes qui ont été prises.
- Corrigez tout renseignement personnel inexact ou modifiez les politiques et les procédures à la lumière du résultat de l'instruction des plaintes.

Conseils

- La façon dont votre organisation traite les plaintes déposées par les particuliers peut contribuer à préserver ou à rétablir la confiance de l'intéressé envers votre organisation.
- Consignez toutes les décisions pour assurer une application uniforme de la Loi.

Exceptions aux principes du consentement et de l'accès

La Loi renferme un certain nombre d'exceptions à l'obligation d'obtenir le consentement et d'assurer l'accès.

Exceptions au principe du consentement énoncées à l'article 7

L'organisation ne peut *recueillir* de renseignements personnels à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

- la collecte de renseignements est manifestement dans l'intérêt de l'intéressé, et le consentement ne peut être obtenu auprès de celui-ci en temps opportun;
- la collecte effectuée au su ou avec le consentement de l'intéressé pourrait compromettre l'exactitude des renseignements ou l'accès à ceux-ci et la collecte est nécessaire à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;
- la collecte est faite uniquement à des fins journalistiques, artistiques ou littéraires;
- il s'agit de renseignements complémentaires auxquels le public a accès.

L'organisation ne peut *utiliser* de renseignements personnels à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

- l'organisation a des motifs raisonnables de croire que les renseignements pourraient être utiles à une enquête sur une contravention au droit fédéral, provincial ou étranger et l'utilisation est faite aux fins d'enquête;
- l'utilisation est faite pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité de tout individu;
- l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites (l'organisation informe le Commissaire à la protection de la vie privée avant d'utiliser les renseignements);
- il s'agit de renseignements complémentaires auxquels le public a accès;
- l'utilisation des renseignements est manifestement dans l'intérêt de l'intéressé, et le consentement ne peut être obtenu auprès de celui-ci en temps opportun;
- la collecte effectuée au su ou avec le consentement de l'intéressé pourrait compromettre l'exactitude des renseignements ou l'accès à ceux-ci et la collecte est nécessaire à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial.

L'organisation ne peut *communiquer* de renseignements personnels à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

- la communication est faite à un avocat qui représente l'organisation;
- elle est faite en vue du recouvrement d'une créance que celle-ci a contre l'intéressé;
- elle est exigée par assignation, mandat ou ordonnance d'un tribunal ou d'un organisme investi des pouvoirs requis;
- elle est faite à une institution gouvernementale qui a demandé à obtenir les renseignements en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application, qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales ou qu'elle est demandée pour l'application du droit canadien ou provincial;
- elle est faite, à l'initiative de l'organisation, à un organisme d'enquête nommé dans le règlement d'application ou à une institution gouvernementale, et l'organisation a des motifs de croire que les renseignements sont afférents à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger ou soupçonne que les renseignements sont afférents à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;
- elle est faite par un organisme d'enquête et est relative à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;
- elle est faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne (l'organisation informe l'intéressé de la communication);
- elle est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites (l'organisation doit informer le Commissaire à la protection de la vie privée avant de communiquer les renseignements);

- elle est faite à une institution qui s'occupe d'archivage;
- elle est faite 20 ans ou plus après le décès de l'intéressé ou 100 ans ou plus après la création du document;
- il s'agit de renseignements complémentaires auxquels le public a accès;
- elle est exigée par la Loi.

Exceptions au principe de l'accès défini à l'article 9:

L'organisation *doit* refuser à un particulier l'accès à des renseignements personnels le concernant lorsque : ▲

- la communication révélerait des renseignements personnels se rapportant à un tiers *, à moins que le tiers en question y consente ou qu'il s'agisse d'une situation qui mette en danger la vie d'une personne;
- l'organisation a communiqué des renseignements personnels à une institution gouvernementale pour des motifs liés à l'application de la loi ou à la sécurité nationale. Sur demande, l'institution gouvernementale peut enjoindre à l'organisation de refuser l'accès aux renseignements ou encore de ne pas divulguer les renseignements qui ont été communiqués. L'organisation peut refuser la demande et informer le Commissaire à la protection de vie privée. L'organisation ne peut informer le particulier de la communication à l'institution gouvernementale, ni du fait que l'institution a été informée de la demande, ni du fait que le Commissaire a été informé du refus.

L'organisation *peut* refuser l'accès à des renseignements personnels si ces derniers appartiennent à l'une ou l'autre des catégories suivantes :

- les renseignements sont protégés par le secret professionnel liant l'avocat à son client;
- la communication révélerait des renseignements commerciaux confidentiels *
- elle risquerait de nuire à la vie ou à la sécurité d'un autre individu *
- les renseignements ont été recueillis à l'insu ou sans le consentement du particulier pour en assurer l'exactitude ou l'accès, et la collecte est nécessaire à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial (le Commissaire doit être informé);
- les renseignements ont été fournis uniquement à l'occasion d'un règlement officiel des différends.

* Si ces renseignements peuvent être supprimés, l'organisation est tenue de communiquer les renseignements restants.

Rôle du Commissaire à la protection de la vie privée

▲

Le Commissaire à la protection de la vie privée du Canada est chargé de la surveillance de la *Loi sur la protection des renseignements personnels* et de la Partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Ces lois protègent les renseignements personnels selon des principes et des pratiques de traitement équitable des renseignements reconnus sur le plan international.

Le Commissaire est un mandataire du Parlement, au même titre que le Vérificateur général du Canada ou le Directeur général des élections. À titre de mandataire du Parlement, le Commissaire relève directement de la Chambre des communes et du Sénat, et non du gouvernement en place. Grâce à cette indépendance, le Commissaire peut faire preuve d'impartialité et d'ouverture dans l'exercice de ses fonctions d'ombudsman pour des questions liées à la protection des renseignements personnels. Le Commissaire n'émet pas d'ordonnance : il formule des recommandations. En vertu d'une disposition de la Loi, il est cependant possible de confier à la Cour fédérale l'examen d'un cas.

Le Commissaire à la protection de la vie privée : ombudsman des questions relatives à la protection des renseignements personnels

Près de deux décennies d'expérience dans l'instruction des plaintes déposées en application de la *Loi sur la protection des renseignements personnels* ont contribué à définir le rôle d'ombudsman du Commissaire à la protection de la vie privée. Ce dernier mise sur la compétence, les connaissances et l'impartialité des membres de son personnel pour, quand la chose est possible, régler les différends au moyen d'enquêtes, de la persuasion, de la médiation et de la conciliation. Idéalement, une telle approche à l'égard du règlement des différends se révèle moins intimidante pour le plaignant et moins coûteuse pour les entreprises que les recours devant les tribunaux. S'il est chargé de la protection des droits des particuliers, le Commissaire défend les principes de l'équité dans le traitement des renseignements qui sont à la base du texte de loi. L'impartialité du

Commissaire et les enquêtes poussées qu'il mène protègent les droits des particuliers et mettent l'organisation à l'abri des accusations injustes.

Responsabilités précises aux termes de la Loi

La Loi confère au Commissaire la responsabilité de l'application de la Loi et de la promotion de ses objectifs.

Rôles en matière de respect

Le Commissaire dispose de cinq moyens pour faire en sorte que les organisations visées par la Loi respectent les principes qui y sont énoncés :

- l'instruction des plaintes;
- la médiation et la conciliation;
- la vérification des pratiques de gestion des renseignements personnels;
- la dénonciation des cas d'abus;
- les recours devant les tribunaux.

(Voir Plaintes devant le Commissaire à la protection de la vie privée, et Vérifications des pratiques de gestion des renseignements personnels)

Promotion des objectifs de la Loi

Le Commissaire fait la promotion des objectifs de la Loi de quatre façons :

- l'éducation;
- la recherche;
- la présentation de rapports;
- la consultation et la conclusion d'ententes.

Éducation

En ce qui concerne l'éducation, le mandat du Commissaire comprend notamment l'élaboration et l'exécution de programmes de sensibilisation du public visant à encourager et à promouvoir la compréhension des questions relatives à la protection des renseignements personnels.

Recherche

La Loi oblige le Commissaire à entreprendre et à publier des recherches sur la protection des renseignements personnels de façons à accroître les connaissances et à favoriser le respect des principes d'équité dans le traitement des renseignements qui sont définis dans la Loi. Le Commissaire peut réaliser des recherches indépendantes sur des questions relatives à la protection des renseignements privés en collaboration avec des universitaires ou d'autres chercheurs. Il peut également accorder des subventions et des contributions à des projets de recherche universitaires ou autres consacrés à de telles questions.

Présentation de rapports

Le Commissaire peut rendre publique de l'information sur les pratiques de gestion des renseignements personnels d'une organisation s'il estime qu'une telle mesure est dans l'intérêt du public. Chaque année, il rend compte au Parlement des questions relatives à la protection des renseignements personnels, notamment en ce qui concerne les provinces qui ont adopté des dispositions législatives analogues.

Consultation et conclusion d'ententes

Le Commissaire peut conclure des ententes avec des homologues provinciaux ayant des pouvoirs et des fonctions analogues.

Ces consultations et ententes peuvent porter sur des mécanismes d'instruction des plaintes, des recherches et l'élaboration de contrats types aux fins de la protection des renseignements personnels. Le Commissaire encouragera les organisations à élaborer des politiques et des pratiques détaillées grâce auxquelles elles se conformeront à la Partie 1 de la Loi.

Plaintes devant le Commissaire à la protection de la vie privée

▲

Types de plaintes

Tout intéressé peut déposer auprès du Commissaire une plainte relativement aux questions mentionnées aux articles 5 à 10 de la Loi ainsi qu'aux recommandations ou obligations définies dans l'Annexe 1. Il peut notamment s'agir d'allégations selon lesquelles une organisation :

- refuse à un particulier l'accès à des renseignements personnels le concernant;
- recueille, utilise ou communique des renseignements personnels de façon impropre;
- refuse de corriger les renseignements inexacts ou incomplets;
- omet de donner accès à des renseignements personnels sur un support de substitution pour un particulier atteint d'une déficience sensorielle;
- ne prend pas les mesures de sécurité qui s'imposent pour assurer la protection des renseignements personnels.

S'il a des motifs raisonnables de croire qu'une enquête se justifie aux termes de la Partie 1 de la Loi, le Commissaire peut lui-même prendre l'initiative d'une plainte.

Délais

Il est possible de déposer en tout temps la plupart des types de plaintes.

La seule exception concerne les plaintes déposées par des personnes à qui on a refusé l'accès aux renseignements personnels les concernant. Dans ce cas, la plainte doit être déposée dans les six mois suivant le refus de l'organisation de fournir les renseignements ou à l'expiration du délai prévu pour la réponse à une demande (pour plus de renseignements sur les délais qui s'appliquent à la réponse à une demande, voir Accès aux renseignements personnel du présent guide). Cependant, le Commissaire peut proroger le délai prévu pour une plainte relative au droit d'accès.

Le Commissaire dispose d'une année à compter de la date du dépôt de la plainte pour préparer un rapport.

Comment le Commissaire à la protection de la vie privée traite-t-il les plaintes?

En sa qualité d'ombudsman, le Commissaire, dans ses enquêtes, adopte le plus souvent possible une approche axée sur la coopération et la conciliation. Il encourage le règlement des plaintes au moyen de la négociation et de la persuasion. À tous les stades de l'enquête, on peut faire appel à de nouvelles méthodes de règlement des différends, par exemple la médiation et la conciliation. Même s'il a le pouvoir de contraindre des témoins à comparaître devant lui, de faire prêter serment et d'exiger la production de preuves, le Commissaire ne se prévaut de ces mesures que lorsque les parties ne collaborent pas volontiers.

Au début d'une enquête, le Commissaire informe l'organisation par écrit du contenu de la plainte et désigne l'enquêteur chargé de l'affaire. En tout temps, l'organisation peut présenter des observations au Commissaire.

L'enquêteur chargé de l'affaire communique avec le membre du personnel de l'organisation désigné pour lui indiquer comment il entend procéder et, le cas échéant, lui préciser les documents dont il aura besoin de même que les membres du personnel qu'il devra interroger. L'enquêteur peut également mentionner si des visites sur place se révéleront nécessaires.

L'enquêteur peut obtenir de l'information directement auprès de personnes qui connaissent bien la question à l'étude. Ces entrevues s'effectuent en privé. L'enquêteur peut également exiger de consulter les documents originaux. Les documents remis à un enquêteur sont retournés dans les dix jours suivant une demande en ce sens, mais l'enquêteur pourra les demander de nouveau s'il en a besoin.

Avant la conclusion de l'enquête, les résultats sont communiqués aux parties en cause. Si elles le souhaitent, ces dernières peuvent faire de nouvelles observations. Elle disposent ainsi d'une nouvelle occasion de régler le différend avant que l'instruction de la plainte ne soit parachevée.

L'enquêteur présente les résultats de l'enquête au Commissaire en même temps que les observations des parties. Le Commissaire étudie la question et présente un rapport aux parties. Le Commissaire peut exiger qu'une organisation lui présente, dans un délai donné, les mesures qu'elle a prises ou qu'elle se propose de prendre pour donner suite aux recommandations du rapport ou encore pour expliquer pourquoi aucune mesure n'a été ou ne sera prise. Le rapport fait également état des résultats de l'enquête, du règlement auquel les parties en sont arrivées, des recommandations, par exemple des modifications proposées aux pratiques de gestion des renseignements, les mesures que l'organisation a prises ou prendra pour donner suite aux recommandations et, le cas échéant, un avis de recours devant la Cour fédérale.

L'étude d'une plainte débouche sur l'un ou l'autre de trois scénarios suivants :

1. La plainte n'est pas fondée

Rien ne permet au Commissaire de conclure que l'organisation a contrevenu à la Loi.

2. La plainte est fondée

L'enquête a montré que l'organisation a contrevenu à une disposition de la Loi et que la plainte n'a pas été réglée.

3. La plainte est réglée

L'enquête confirme le bien-fondé de la plainte, mais l'organisation accepte de prendre des mesures correctives pour remédier à la situation. Par exemple, elle accepte de communiquer des renseignements personnels auxquels elle avait au préalable refusé l'accès.

On peut également considérer la plainte comme réglée si elle résulte d'un malentendu ou d'une mauvaise communication. Par exemple, il est possible qu'une organisation ait mal compris le sens de la demande et qu'elle accepte de communiquer les renseignements personnels demandés par le plaignant.

La plainte peut également être considérée comme réglée si le plaignant est satisfait des efforts du Commissaire et des résultats.

Le Commissaire n'est pas tenu de produire un rapport d'enquête si :

- le plaignant n'a pas cherché à exercer d'autres recours qui s'offent à lui;
- l'affaire pourrait être traitée de façon plus efficace au moyen d'un autre texte de loi;
- trop de temps s'est écoulé depuis que le problème à l'origine de la plainte s'est produit, si bien que la préparation d'un rapport ne servirait à aucune fin utile;
- la plainte est futile, vexatoire ou entachée de mauvaise foi.

Communication publique

Le Commissaire à la protection de la vie privée peut rendre publique toute information concernant les pratiques de gestion des renseignements personnels d'une organisation s'il estime que la mesure est dans l'intérêt du public.

Recours devant la Cour fédérale

▲

Tout plaignant peut demander à être entendu par la Cour fédérale. Le Commissaire à la protection de la vie privée peut lui-même demander une audience au nom d'un plaignant. Normalement, les demandes en ce sens doivent être présentées dans les 45 jours suivant le dépôt du rapport du Commissaire.

Les affaires qui peuvent être entendues

La Cour considérera les demandes de recours découlant de la plainte ou toute question mentionnée dans le rapport du Commissaire et portant sur l'un ou l'autre des points suivants.

Annexe 1

4.1.3 L'organisation s'est-elle acquittée comme il se doit de la responsabilité qui lui échoit à l'égard des renseignements personnels qu'elle a en sa possession, y compris les renseignements confiés à une tierce partie?

4.2 L'organisation a-t-elle correctement défini et documenté les fins auxquelles les renseignements sont recueillis, utilisés ou communiqués avant ou pendant la collecte?

4.3.3 L'organisation a-t-elle refusé d'accorder un service à un particulier pour le motif que ce dernier n'a pas consenti à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour les fins précisées?

4.4 L'organisation a-t-elle recueilli plus de renseignements que ceux qui sont nécessaires aux fins déterminées? Les renseignements en question ont-ils été recueillis de façon honnête et licite?

4.6 Les renseignements personnels sont-ils aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés?

4.7 L'organisation a-t-elle pris les mesures nécessaires pour assurer la sécurité des renseignements?

4.8 L'organisation a-t-elle fait en sorte que des renseignements précis sur ses politiques de gestion des renseignements personnels soient facilement accessibles à toute personne?

Annexe 1 telle que modifiée par les articles 5 à 10 de la Loi

4.3 Les renseignements personnels ont-ils été recueillis, utilisés ou communiqués à l'insu de l'intéressé ou sans son consentement, sauf lorsque la Loi le permet ou l'exige?

4.5 L'organisation a-t-elle utilisé ou communiqué des renseignements personnels à des fins autres que celles auxquelles ils étaient destinés, sans le consentement de l'intéressé et sans que la loi le permette? De même, l'organisation a-t-elle conservé les renseignements pendant le temps voulu pour que le plaignant se prévale des recours prévus par la Loi?

4.9 A-t-on injustement refusé à un particulier l'accès à des renseignements le concernant, sauf lorsque la Loi le permet ou l'exige?

Dispositions de la Loi

5(3) Les renseignements ont-ils été recueillis, utilisés ou communiqués uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances?

8(6) A-t-on imposé à un particulier des droits trop élevés pour l'accès aux renseignements? A-t-il été informé du coût au préalable?

8(7) L'organisation a-t-elle informé l'intéressé par écrit de son refus d'acquiescer à la demande? A-t-elle présenté les motifs du refus et informé le demandeur des recours qui s'offrent à lui?

10 L'organisation a-t-elle omis d'accorder l'accès sur un support de substitution à une personne atteinte d'une déficience sensorielle?

Redressements offerts par la Cour fédérale

La Cour fédérale peut ordonner à une organisation de corriger des pratiques non conformes aux articles 5 à 10 de la Loi. Elle peut aussi ordonner à une organisation de publier un avis faisant état des mesures prises ou proposées pour corriger les pratiques concernées. Enfin, elle peut accorder au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie. Il n'y a aucune limite aux dommages pécuniaires que la Cour peut accorder.

Vérifications des pratiques de gestion des renseignements personnels

La Loi confère au Commissaire à la protection de la vie privée le pouvoir de vérifier les pratiques de gestion des renseignements personnels d'une organisation lorsqu'il a des motifs raisonnables de croire que cette dernière ne s'acquitte pas de ses obligations aux termes de la Partie 1 de la Loi ou qu'elle ne se conforme pas aux recommandations énoncées à l'Annexe 1.

Circonstances pouvant conduire à une vérification

On trouvera ci-après des exemples de circonstances pouvant amener le Commissaire à vérifier les pratiques de gestion des renseignements personnels d'une organisation :

- un groupe ou une série de plaintes à propos des pratiques d'une organisation donnée;
- des renseignements fournis par un particulier aux termes de la disposition relative à la dénonciation;
- toute question retenant l'attention des médias.

Qu'attendre d'une vérification effectuée par le Commissaire?

Conformément au rôle d'ombudsman du Commissaire, les vérifications relatives à la protection des renseignements personnels sont, dans la mesure du possible, non conflictuels. Ces vérifications peuvent se révéler utiles pour les organisations souhaitant améliorer leurs pratiques en matière de traitement des renseignements personnels.

Le Commissaire informe par écrit l'organisation de ce qu'une vérification sera menée. Dans la lettre, le Commissaire précise la portée de la vérification, propose un calendrier raisonnable et nomme le mandataire chargé de la vérification.

Même s'il a le pouvoir de contraindre des témoins à comparaître devant lui, de faire prêter serment et d'obliger des organisations à produire des preuves, le Commissaire n'effectuera vraisemblablement pas les vérifications de façon aussi officielle, à moins que les parties ne collaborent pas volontiers.

Le mandataire rencontrera le représentant de l'organisation pour discuter de façon préliminaire de l'intention, de l'objet et de la portée de l'examen.

Lorsqu'il demande d'avoir accès à des locaux de l'organisation, le mandataire inspectera les mesures de sécurité. Sur place, il peut interroger toute personne en privé, examiner les dossiers, obtenir des copies de tel dossier ou en prélever des extraits. Le mandataire retournera les documents dans un délai de 10 jours suivant une demande en ce sens. Il pourra les demander de nouveau s'il en a besoin.

Une fois la vérification terminée, le mandataire informera le représentant de l'organisation de ses conclusions. Il fera état de ses résultats au Commissaire, qui formulera des recommandations. Le Commissaire fera parvenir le rapport à l'organisation et pourra demander à être tenu au courant des mesures prises par l'organisation pour corriger les problèmes.

Le Commissaire peut inclure le rapport de vérification dans son rapport annuel ou rendre publiques les pratiques de gestion des renseignements personnels d'une organisation s'il estime que la mesure est dans l'intérêt du public.

Questionnaire sur la protection des renseignements personnels

▲

Vous trouverez ci-après quelques questions de bon sens que vous pouvez vous poser pour aider votre organisation à se préparer en vue de la mise en oeuvre de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Vous pouvez utiliser le questionnaire qui suit parallèlement à la description de la Loi que renferme le présent guide.

Si vous n'êtes pas certain que votre organisation est visée par la Loi, consultez Votre organisation est-elle visée par la Loi? du guide.

Comme la Loi s'applique à des organisations de types et de tailles divers, les questions qui suivent ne s'appliqueront pas à toutes. Étudiez chacune des questions à la lumière des pratiques actuelles de votre organisation. Le fait de répondre « non » dénote qu'il s'agit d'un problème à régler ou d'un aspect à améliorer.

Banques de renseignements personnels

- Savez-vous ce que sont des renseignements personnels?
- Recueillez-vous, utilisez-vous ou communiquez-vous des renseignements personnels dans vos activités commerciales?
- Avez-vous un répertoire des banques de renseignements personnels que vous avez en votre possession?
- Savez-vous où les renseignements personnels sont emmagasinés (dossiers et lieux matériels)?
- Savez-vous sous quelle(s) forme(s) les renseignements personnels sont emmagasinés (support électronique, support papier, etc.)?
- Savez-vous qui a accès aux renseignements personnels, à l'intérieur et à l'extérieur de votre organisation?

Responsabilité de l'organisation et des employés

- Avez-vous désigné un mandataire des questions relatives à la protection des renseignements privés chargé du respect de la Loi par votre organisation?
- La responsabilité est-elle assumée par plus d'une personne?
- Si la responsabilité est partagée, les fonctions ont-elles été clairement définies?
- Vos employés sont-ils en mesure de répondre à des questions de l'intérieur et de l'extérieur concernant la protection des renseignements personnels au nom de l'organisation? Sinon, savent-ils qui devrait y répondre?
- Vos employés savent-ils qui reçoit :
  - les demandes relatives aux renseignements personnels?
  - les demandes de correction?
  - les plaintes émanant du public?
- Vos clients savent-ils avec qui communiquer pour :
  - présenter des demandes de renseignements généraux sur les renseignements personnels les concernant?
  - demander accès aux renseignements personnels les concernant?
  - demander que des modifications soient apportées aux renseignements personnels les concernant?
  - porter plainte?
- Le mandataire responsable de la protection des renseignements personnels est-il en mesure d'expliquer aux membres du public les étapes et les procédures à suivre pour demander accès à des renseignements personnels et pour porter plainte?
- Vos employés ont-ils été initiés à la Loi?
- Allez-vous assurer une formation constante?
- Vos employés sont-ils en mesure d'expliquer aux clients, de façon intelligible, les fins auxquelles la collecte, l'utilisation et la communication des renseignements personnels sont destinées?
- Vos employés sont-ils en mesure d'expliquer aux clients le moment où et la façon dont ils pourront retirer leur consentement et quelles seront, le cas échéant, les conséquences d'un tel retrait?
- Informerez-vous vos employés des nouvelles questions relatives à la protection des renseignements personnels que soulèvent les changements technologiques, les examens internes, les plaintes du public et les décisions des tribunaux?

Information pour les clients et les employés

- Avez-vous des documents qui expliquent à vos clients vos procédures et pratiques relatives aux renseignements

personnels?

- Y trouve-t-on de l'information sur les moyens :
  - d'obtenir des renseignements personnels?
  - de corriger des renseignements personnels?
  - de présenter une demande de renseignements ou de déposer une plainte?
- Y décrit-on les renseignements personnels :
  - que possède l'organisation et l'utilisation qui en est faite?
  - communiqués aux filiales et à d'autres parties?
- Avez-vous élaboré une politique relative à la protection des renseignements personnels pour votre site Web?
- Votre politique relative à la protection des renseignements personnels est-elle visible et facile à trouver? Est-elle facile à comprendre?
- Dans vos formulaires de demande, questionnaires, formulaires d'enquête, dépliants et brochures, expliquez-vous clairement les fins auxquelles la collecte, l'utilisation et la communication de renseignements personnels sont destinées?
- Avez-vous passé en revue tous vos documents d'information du public pour vous assurer que les sections portant sur les renseignements personnels sont claires et compréhensibles?
- Avez-vous pris des mesures pour que le public puisse obtenir ces renseignements facilement et gratuitement?
- Examinez-vous périodiquement les renseignements pour vous assurer qu'ils sont exacts, complets et à jour?
- Les renseignements incluent-ils le nom ou le titre actuel de la personne responsable de la surveillance du respect de la Loi?

Limitation de la collecte, de l'utilisation, de la communication et de la conservation aux fins mentionnées

- Avez-vous défini les fins auxquelles la collecte de renseignements personnels est destinée?
- Les fins sont-elles définies au moment de la collecte de renseignements ou avant?
- Ne recueillez-vous des renseignements personnels qu'aux fins mentionnées?
- Documentez-vous les fins auxquelles des renseignements personnels sont recueillis?
- Si vous recueillez et combinez des renseignements personnels provenant de plus d'une source, vous assurez-vous que les fins initiales n'ont pas changé?
- Avez-vous élaboré un calendrier aux fins de la conservation et de la suppression des renseignements personnels?
- Lorsque les renseignements personnels ne sont plus utiles aux fins mentionnées ou qu'ils ne sont plus prescrits par la loi, vous assurez-vous de les détruire, de les effacer ou de les rendre anonymes?

Consentement

- Vos employés savent-ils qu'ils doivent obtenir le consentement de l'intéressé au moment de recueillir des renseignements personnels le concernant ou avant?
- Vos employés savent-ils qu'ils doivent obtenir le consentement de l'intéressé avant toute nouvelle utilisation ou communication des renseignements?
- Avez-vous recours au consentement explicite chaque fois qu'il est possible de le faire et en tout temps lorsque les renseignements sont délicats ou que l'intéressé est raisonnablement en droit de s'attendre à ce qu'il en soit ainsi?
- La formule de consentement que vous utilisez est-elle libellée de façon claire, de manière que l'intéressé comprenne la fin à laquelle la cueillette, l'utilisation ou la communication est destinée?
- Précisez-vous clairement aux clients qu'ils ne sont pas tenus de fournir des renseignements personnels autres que ceux qui sont essentiels aux fins de la cueillette, de l'utilisation ou de la communication?

Tierces parties

- Utilisez-vous des contrats pour assurer la protection des renseignements personnels confiés à une tierce partie aux fins de traitement?
- Le contrat limite-t-il l'utilisation que la tierce partie peut faire des renseignements aux fins nécessaires à l'exécution du contrat?
- Le contrat oblige-t-il la tierce partie à vous transmettre toute demande de consultation ou toute plainte concernant les renseignements qui vous ont été communiqués?
- Le contrat précise-t-il le moment où et la façon dont une tierce partie doit supprimer ou retourner les documents personnels qu'elle reçoit?

Exactitude

- Les renseignements personnels sont-ils suffisamment exacts, complets et à jour pour réduire au minimum les risques d'utilisation inappropriée par votre organisation?
- Votre organisation documente-t-elle le moment où et la façon dont les renseignements personnels sont mis à jour de façon à en assurer l'exactitude?
- Veillez-vous à ce que les renseignements personnels communiqués par une tierce partie soient exacts et complets?

Mesures de sécurité

- Avez-vous examiné vos mesures de sécurité matérielle, technologique et administrative?
- Ces mesures préviennent-elles la modification, la cueillette, l'utilisation, la communication ou la suppression inadéquate des renseignements personnels ou les accès impropres à ces derniers?
- Les renseignements personnels sont-ils protégés par des mesures de sécurité proportionnelles :
  - au caractère délicat des renseignements?
  - à l'importance de leur distribution?
  - au support sur lesquels ils sont présentés?
  - à la méthode d'emmagasinage?
- Avez-vous mis au point un critère sélectif pour limiter l'accès aux renseignements personnels au droit de savoir?
- Avez-vous initié les membres de votre personnel aux pratiques de sécurité visant à assurer la protection des renseignements personnels? Par exemple, vos employés savent-ils qu'aucun renseignement personnel ne devrait rester affiché sur leur écran d'ordinateur ou leur bureau en leur absence?
- Vos employés savent-ils qu'ils doivent s'assurer de l'identité des intéressés et établir leur droit d'accès aux renseignements personnels avant de communiquer ces derniers?
- Avez-vous établi des règles concernant les personnes autorisées à ajouter, à modifier ou à effacer des renseignements personnels?
- Disposez-vous d'un système de gestion des dossiers qui assigne des comptes d'utilisateur, des droits d'accès et des autorisations de sécurité?
- Veillez-vous à ce qu'aucune partie non autorisée ne puisse supprimer des renseignements personnels, y avoir accès, les modifier ou les détruire?

Demandes de communication de renseignements personnels

- Vos employés sont-ils au fait des délais autorisés par la Loi pour les réponses aux demandes de communication?
- Pouvez-vous extraire des renseignements personnels pour répondre à des demandes de communication tout en réduisant au minimum les interruptions de vos activités?
- Vos systèmes d'information facilitent-ils l'extraction et la description exactes des renseignements personnels concernant un intéressé, y compris les communications à des tierces parties?
- Fournissez-vous les renseignements personnels à l'intéressé gratuitement ou à un coût minimal?
- Le cas échéant, informez-vous l'auteur de la demande des coûts avant l'extraction des renseignements personnels?
- Consignez-vous par écrit la réponse de l'intéressé après que ce dernier a été informé du coût de l'extraction des renseignements personnels?
- Présentez-vous les renseignements personnels dans une forme généralement compréhensible? (Par exemple, expliquez-vous les abréviations?)
- Votre organisation dispose-t-elle de procédures pour répondre aux demandes de renseignements personnels sur support de substitution (par exemple le braille ou les bandes audio)?

Instruction des plaintes

- Un particulier peut-il facilement déterminer la marche à suivre pour déposer une plainte auprès de vous?
- Traitez-vous les plaintes dans les délais?
- Instruisez-vous toutes les plaintes reçues?
- Vos préposés au service à la clientèle et autres employés de première ligne sont-ils en mesure de faire la distinction entre une plainte déposée aux termes de la Loi et une demande de renseignements généraux? Dans le doute, en discutent-ils avec l'intéressé?
- Informez-vous les intéressés des recours qui s'offrent à eux, notamment auprès du Commissaire à la protection de la

vie privée?

- Examinez-vous les suites données par vos employés aux demandes de renseignements du public, aux demandes de communication et aux plaintes pour vous assurer que celles-ci sont équitables, exactes et rapides?
- Lorsqu'une plainte est fondée, prenez-vous les mesures correctives qui s'imposent, par exemple la modification des politiques et la communication des résultats aux employés?

CLOSE